VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

OCHRANA OSOBNÍCH ÚDAJŮ U POSKYTOVATELE HOSTINGU
PERSONAL DATA PROTECTION IN A HOSTING PROVIDER

BAKALÁŘSKA PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — **Sára Juricová**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. Viktor Ondrák, Ph.D.**
SUPERVISOR

BRNO 2021

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání bakalářské práce

Ústav:	Ústav informatiky
Studentka:	**Sára Juricová**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Manažerská informatika
Vedoucí práce:	**Ing. Viktor Ondrák, Ph.D.**
Akademický rok:	2020/21

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává bakalářskou práci s názvem:

Ochrana osobních údajů u poskytovatele hostingu

Charakteristika problematiky úkolu:

Úvod
Vymezení problému a cíle práce
Analýza současného stavu
Teoretická východiska práce
Vlastní návrhy řešení
Závěr
Seznam použité literatury
Přílohy

Cíle, kterých má být dosaženo:

Navrhnout systém ochrany osobních údajů.

Základní literární prameny:

BARTÍK, Václav a Eva JANEČKOVÁ. Ochrana osobních údajů v životě podnikatele: 103 řešení modelových situací. Olomouc: ANAG, 2013. ISBN 978-80-7263-811-6.

DOSEDĚL, Tomáš. 21 základních pravidel počítačové bezpečnosti. Brno: CP Books, 2005. ISBN 80-2510-574-1.

KNAP, Karel. Ochrana osobnosti podle občanského práva. 4. dopl. vyd. Praha: Linde, 2004. ISBN 80-7201-484-6.

MATES, Pavel, Eva JANEČKOVÁ a Václav BARTÍK. Ochrana osobních údajů. Praha: Leges, 2012. ISBN 978-80-87576-12-0.

MATOUŠOVÁ, Miroslava a Ladislav HEJLÍK. Osobní údaje a jejich ochrana. 2. dopl. vyd. Praha: ASPI, 2008. ISBN 80-7357-322-9.

Termín odevzdání bakalářské práce je stanoven časovým plánem akademického roku 2020/21

V Brně dne 28.2.2021

L. S.

.....	.....
Mgr. Veronika Novotná, Ph.D. ředitelka	doc. Ing. Vojtěch Bartoš, Ph.D. děkan

Abstrakt

Táto bakalárska práca sa sústredí na ochranu osobných údajov vo firme, ktorá poskytuje registráciu domén a hosting. Pôjde o analýzu možných stretov s osobnými údajmi ako zákazníkov, uchádzačov o zamestnanie a obchodných partnerov, a bude sa opierať o nové zákony o ochrane osobných údajov, ktoré sa implementujú do vnútorných predpisov firmy tak, aby nebola právne napadnuteľná.

Abstract

This bachelor thesis focuses on personal data protection in a company that provides domain registration and hosting. It will be an analysis of possible encounters with personal data of customers. job seekers and business partners, and it will rely on the new laws on personal data protection and implement them into the company's internal regulations so that it is not legally challengeable.

Kľúčové slová

GDPR, zákon č. 18/2018 Z. z., zákon o ochrane osobných údajov, hosting, domény, firma, poskytovateľ služieb

Keywords

GDPR, Act no. 18/2018 Coll., Personal Data Protection Act, hosting, domains, company, service provider

Bibliografická citace

JURICOVÁ, Sára. *OCHRANA OSOBNÍCH ÚDAJŮ ZE STRANY POSKYTOVATELE HOSTINGU*. Brno, 2021. Dostupné také z: https://www.vutbr.cz/studenti/zav-prace/detail/132938. Bakalářská práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Viktor Ondrák.

Čestné prehlásenie

Úprimne prehlasujem, že táto bakalárska práca je v pôvodnom znení a spracovala som ju samostatne. Zároveň prehlasujem, že citácia predložených zdrojov je úplná a vo svojej práci som vedome neporušila žiadne autorské práva (podľa Zákona č. 185/2015 Z. z. Autorský zákon).

_____

podpis študenta

Poďakovanie

Moje ďakujem patrí vedúcemu práce, pánovi Ing. Viktorovi Ondrákovi, PhD., za správne nasmerovanie a ochotu, informácie a rady. Naďalej JUDr. Patrícii Scholczovej, MBL a firme, ktorá mi umožnila použiť jej dáta na dokončenie tejto práce.

OBSAH

ÚVOD

Žijeme v 21. storočí. Mnohí túto éru označujú ako informačnú. História je plná informácii. Každá udalosť nám priniesla dáta, ktoré bolo potrebné spracovať tak, aby sa z nich stali informácie. Informácie dôležité pre ďalšie plánovanie v budúcnosti. Stali sa teda cennou zložkou, či už pri komunikácii, pri vývoji, alebo pri obchodovaní. Obchodovanie s informáciami však v 21. storočí naberá rýchly spád a kvôli technickým pokrokom sa mení aj celá naša spoločnosť a využívanie ich informácii v internetovom priestore. Je prirodzené, že náš životný štýl a množstvo osobných informácii sa odlišuje od štýlu pred pár desiatkami rokov, dôležité je však, vedieť si tieto informácie aj patrične ochrániť. Technológie nás ovplyvňujú viac, než by sme niekedy chceli a preto je potrebné chrániť seba a svoje súkromie reguláciami.

Osobné dáta sa stali najobchodovateľnejším a najdrahším produktom tejto doby. Denne sa vystavujeme desiatkam tretích strán, ktoré čakajú len na to, aby sa o nás a o našich preferenciách dozvedeli čo najviac. Následne zozbierané dáta predávajú ďalej firmám, ktoré pomocou našich preferencii vedia svižne a efektívne obrátiť marketing a zacieliť reklamu, produkt alebo služby tak, aby nás nevedomky ovplyvnili si ich produkt kúpiť, kliknúť naň, alebo rozposlať ďalej. Čím viacej týchto informácii majú, tým lepšie ich vedia zacieliť na potencionálnych zákazníkov a budovať si tým lepšiu pozíciu na trhu. Spotrebiteľ (zákazník) je častokrát nevzdelaný a neuvedomuje si tieto udalosti prebiehajúce za oponou webovej stránky. Preto bolo potrebné aby štát reguloval tento priestor nariadením o ochrane osobných údajov (informácii).

V roku 2018, Európsky parlament vydal všeobecne nariadenie o ochrane osobných údajov, ktoré nadobudlo platnosť 25. mája. Podstatou bola ochrana fyzických osôb. Každý, kto zhromažďuje a spracováva tieto údaje – Európanov, vrátane spoločností, a inštitúcii mimo EÚ, takých, ktorý pôsobia na Európskom trhu.

Vymedzenie problému a cieľ práce

Cieľom tejto práce je preveriť aktuálne znenie smernice GDPR firmy poskytujúcej hosting a na základe jej kontroly vytýčiť nedostatočné riešenia a chyby. Aktuálne firma spracováva dáta pre viac ako 20 000 užívateľov, desiatky zamestnancov, obchodných partnerov a návštevníkov webového rozhrania. Preto je nutné, aby pokrývala všetky odvetvia pracujúce s osobnými údajmi a zároveň, aby jej znenie nebolo v právnom rozpore so zákonom. Nie len v smernici, ale aj v praktickej sfére ochrany osobných údajov má firma niekoľko slabých miest v rámci infraštruktúry, pre ktoré je nutné vytvoriť nové opatrenia a aktualizovať staré. Táto práca má za úlohu revidovať všetky možné strety s osobnými údajmi a vytvoriť v nich prostredie s nulovým ohrozením zneužitia osobných údajov. Ako prvý bod bude analýza prostredia a jej tabuľkové zobrazenie spracovania dát. Následne sa vysvetlí teoretický podklad, o ktorý sa bude práca opierať – čo sú to osobné údaje, ako sa delia, spracúvajú a prečo je nutné ich chrániť, rozloženie smernice GDPR a jej zákonnosť na Slovensku - jej nutnosť implementácie a napokon samostatná implementácia do firemného prostredia.

1 ANALÝZA SÚČASNÉHO STAVU

1.1 Základná analýza spoločnosti

Firma, ktorá poskytla konkrétne informácie, nebude z bezpečnostných a právnych dôvodov menovaná. Pre opis aktuálneho stavu je vybrané vymyslené meno a nepravdivé interné informácie.

Pri analýze firmy „Web-net s.r.o.“ z ekonomického hľadiska sú vytýčené tieto základné pojmy:

- **Podnik poskytujúci služby**
  - Podnik poskytujúci doménový názov, internetový priestor a prevádzku emailov.
- **Malý podnik**
  - Podnik má 19 zamestnancov, ročný obrat ≤10 000 000€
  - Podnik zároveň spĺňa kritéria podľa uspokojovania potrieb ako zákazníkov, tak aj iných podnikov, pre ktoré pripravuje podporné služby na ich rozvoj.
- **Súkromný podnik**
  - Majiteľom je fyzická osoba, nepodieľa sa na jeho fungovaní štát.
- **Obchodná spoločnosť**
  - Spoločnosť s ručením obmedzeným - S.R.O.

Firma Web-net s.r.o. je takmer na vrchole slovenského rebríčku poskytovateľov hostingu. Patrí medzi najlepšie slovenské firmy poskytujúce hosting, na konte má až do 50 000 domén. Okrem registrácie vyše 100 doménových koncoviek, emailových služieb, hostingového priestoru poskytuje aj virtuálne (Linux, Windows, Cloud), alebo dedikované servery. Infraštruktúra je distribuovaná v troch geograficky nezávislých dátových centrách, ktoré sú navzájom redundantne prepojené ich vlastnými optickými linkami. Všetky dátové centrá spĺňajú náročné medzinárodné kritériá bezpečnosti a dostupnosti. Konektivitu nakupujú od dvoch dodávateľov na nezávislých miestach. Routujú ju na vlastnom autonómnom IP rozsahu za pomoci zariadení Cisco. Táto architektúra umožňuje byť online aj vtedy, ak je na niektoré dátové centrum vedený DDOS útok. Všetky sieťové zariadenia prevádzkujú minimálne v konfigurácii N+1,

inými slovami – infraštruktúra neobsahuje tzv. „single point of failure“. Pre zabezpečenie najvyššej dostupnosti a škálovateľnosti používajú virtualizačné technológie VMware (cloudová virtualizácia) a HyperV (klasická virtualizácia). [1]

Firma vznikla na základe spojenia dvoch menších poskytovateľov. Kampane siahajú až do Malajzie, avšak plán je rozširovať svoje pôsobenie v Maďarsku a v Čechách. Aktuálne sa posúva pod skupinu XY Group. a.s. pod ktorou figurujú aj ďalšie české a slovenské firmy.

Tabuľka 1 – rozpis členov firmy
(Zdroj: Vlastné spracovanie)

Rozpis členov firmy v priemere za rok		
Zamestnanci	<20*	L1,L2,L3, Marketing, Sales, Vedenie firmy, fakturačné oddelenie...
Partneri	>100*	Uvedení v sekcii obchodný partneri
Uchádzači o zamestnanie	5*	Fyzické osoby z externého prostredia
Zákazníci	>15000*	Fyzické a kontaktné osoby právnických osôb

*Čísla sú fiktívne na žiadosť firmy.

1.2 Subjekty osobných údajov

Firma Web-net s.r.o. uchováva osobné údaje jej klientov / zákazníkov z dôvodu histórie platieb, vedenia databázy zákazníkov, zachovania obchodných zmlúv, v ktorých sa údaje nachádzajú. Ide o fyzické osoby a kontaktné osoby právnických osôb. Subjekty, ktorých osobné údaje firma spracováva, sú rozdelené do nasledujúcich skupín:

- Zamestnanci
- Obchodný partneri / Dodávatelia
- Uchádzači o zamestnanie
- Zákazníci - Klienti
- Iné

Všetky zmluvy sú vedené v Informačnom systéme firmy.

Prevádzkovateľ zabezpečuje bezpečnosť informačných systémov voči potenciálnemu úniku alebo zneužitiu v dôsledku hackerského útoku, ako aj v dôsledku možného rizikového konania zamestnanca spoločnosti prijatím a kontrolou bezpečnostných opatrení. Informačný systém je vedený v zmysle smernice GDPR a Zákona 18/ 2018. Žiadne zo spracovaných údajov nespadajú do kategórie zvláštnych osobných údajov (podľa čl. 9 "Spracúvanie osobitných kategórií osobných údajov"), resp. také, ktoré spadajú, sú ošetrené súhlasom podpísaným pri nástupe do zamestnania, alebo inak vymedzené v osobitnej zmluve.

1.2.1 Zamestnanci

Zamestnanci pri vstupe do zamestnania vypisujú zmluvu o vykonávaní pracovnej činnosti a súhlas so spracovaním osobných údajov. Súhlas je vo forme listiny priloženej ku pracovnej zmluve. (príloha č.1) a súhlas pre spracovanie fotografie ako citlivý obsah (príloha č.2).

Tabuľka 2 - Spracúvanie v IS – zamestnanci
(Zdroj: Vlastné spracovanie)

Informačný systém Interný	
Dotknuté osoby	Zamestnanci
Spracovávané osobné údaje	Uvedené v osobitnej tabuľke.
Účel	Personálna a mzdová agenda
	Právne a regulačné povinnosti
	Hodnotenie, spokojnosť zamestnancov
Príjemca	Zamestnávateľ
Sprostredkovatelia	Zamestnanci osobne
Bezpečnostné opatrenia	Smernica o ochrane osobných údajov
Tretie strany	Nie
Právny základ	Spracovanie nevyhnutné podľa osobitného predpisu alebo medzinárodnej Zmluvy.

Sledované osobné údaje:

Tabuľka 3 - Osobné údaje – Zamestnanci
(Zdroj: Vlastné spracovanie)

Názov osobného udajú	
Identifikačné údaje	● Meno ● Priezvisko ● Rodné priezvisko ● Tituly ● Dátum a miesto narodenia ● Rodné číslo ● Číslo OP ● Bydlisko ● Štátna príslušnosť
Kompetenčné údaje	● Vzdelanie ● Absolvované kurzy ● Certifikáty ● Potvrdenie o zdravotnej spôsobilosti
Údaje pre účely daní, sociálneho a zdravotného poistenia	● Rodinný stav ● Manžel/ka, deti ● Zdravotná poisťovňa, číslo poistenca
Pracovné údaje	● Odpracovaná doba ● Neprítomnosť ● Pracovný výkon
Mzdové údaje	● Mzda ● Číslo účtu (so súhlasom a želaním posielania mzdy na účet)
Osobné, kontaktné údaje	● Číslo ● E-mail
Fotografia	V prípade, že zamestnanec dodal súhlas.(príloha č.2)

Zdroj údajov

Dáta sú získané výhradne od zamestnancov a to v prípade tvorby zmluvy po prijatí do zamestnania a na základe podpísania súhlasu so spracovaním osobných údajov.

Prístup k údajom

Prístupom disponujú riaditelia, zamestnanci vo vedúcich pozíciách a fakturačné oddelenie. K osobným údajom zamestnancov má plný prístup iba najvyššie vedenie, fakturačné oddelenie (v rámci certifikácie hradenej firmou), kde je povinné uviesť meno zamestnanca a jeho poštové údaje.

Vymazanie musí nastať

Podľa § 23 Právo na výmaz osobných údajov – podľa konkrétnych skutočností:

- Po ukončení pracovnej zmluvy – nie sú potrebné pre ďalšie uchovávanie
- Nebol podpísaný súhlas o spracovaní alebo ho zamestnanec odvolá
- Pri porušení pracovnej zmluvy

Dáta Zamestnancov

Osobné dáta zamestnancov sú uložené v samostatnom personálnom systéme, ktorý je doplnený o modul spracovania osobných údajov. V organizácii existujú smernice definujúce všetky vykonávané procesy pri spracovaní týchto údajov a podľa nezávislého auditu sú smernice úplné a splňujú všetky požiadavky kladené na smernice o osobných údajoch. Na základe tohto faktu bolo rozhodnuté neuvádzať ďalší rozbor kategórii zamestnancov v tejto bakalárskej práci.

1.2.2 Uchádzači o zamestnanie

Údaje o uchádzačovi sa v tomto prípade neukladajú do informačného systému, posielajú sa výhradne emailom osobe poverenej na spracovávanie osobných údajov. Po ukončení výberového konania sú životopis a prípadné dokumenty zničené - skartované. Pre jednoduchšiu správu sa bude prostredie uchovávania nazývať Informačným systémom.

Uchádzači sa môžu o ponuke zamestnania dozvedieť:

- Ústnou ponukou na akciách
- Priamo na oficiálnej stránke spoločnosti
- Inzercii na profesia.sk

Tabuľka 4 Spracovanie v IS – uchádzači o zamestnanie
(Zdroj: Vlastné spracovanie)

Informačný Systém uchádzačov o zamestnanie	
Dotknuté osoby	Uchádzači o zamestnanie
Spracovávané osobné údaje	Uvedené v osobitnej tabuľke
Účel	Prijatie na voľnú pozíciu
Príjemcovia	Zodpovedná osoba pre výberové konania
Sprostredkovatelia	Fyzické osoby, Agentúra
Bezpečnostné opatrenia	Smernica o ochrane osobných údajov
Tretie strany	Nie. Prístup má výlučne iba zodpovedná osoba pre uchádzačov.
Právny základ	Spracovanie nevyhnutné podľa osobitného predpisu alebo medzinárodnej zmluvy

Sledované osobné údaje:

Tabuľka 5 - Osobné údaje – uchádzači o zamestnanie
(Zdroj: Vlastné spracovanie)

Názov osobného udajú	
Identifikačné údaje	● Meno ● Priezvisko ● Tituly ● Rodné číslo ● Trvalé Bydlisko ● Štátna príslušnosť
Kompetenčné údaje	● Vzdelanie ● Absolvované kurzy ● Certifikáty
Osobné, kontaktné údaje	● Číslo ● E-mail
Fotografia	V prípade, že uchádzač dodal súhlas.

Zdroj údajov

Dáta sú získané výhradne od uchádzačov o zamestnanie pri fyzickom pohovore, alebo zaslané subjektom formou CV.

Prístup k údajom

Prístup musí mať iba zamestnanec poverený pri výberovom konaní.

Vymazanie musí nastať:

- Po ukončení výberového konania má osoba zodpovedná za výberové konanie povinnosť rozposlať oznam o ukončení takéhoto konania s informáciou o prijatí, resp. neprijatí. Oznam sa rozpošle predom dohodnutou formou, spravidla však emailom. V prípade neprijatia na danú pozíciu obdrží dotknutá osoba oznámenie, že týmto rozhodnutím pominul dôvod pre držanie a spracovanie osobných údajov a tieto údaje budú bezodkladne odstránené.
- Ak sa nedostaví na výberové konanie.

Vymazanie týchto údajov nemusí nastať, pokiaľ bude uchádzač prijatý do zamestnania.

1.2.3 Obchodní partneri / Dodávatelia

Do obchodných partnerov patria všetky zainteresované skupiny, s ktorými má firma podpísanú zmluvu na určité obdobie. Pod zmluvných partnerov patria:

Tabuľka 6 Obchodní partneri
(Zdroj: Vlastné spracovanie)

Zmluvní partneri	
Centrálne registre	SK-NIC, a.s., Gransy, Joker, RRP Proxy
Hardware	DELL
Software	Licencie Microsoft, CloudLinux,Worpdress,Joomla a pod.
SSL certifikáty	Subreg.cz , sslmarket.sk,thawte.com, godaddy.com

Úschovňa serverov	SWAN a Telekom
Telefóny	O2 Slovensko
Vzdelanie	Easy-Academy
Certifikácie	AWS Cloud GURU
Právnická služba	ProActive s.r.o
Priestor	A-S Reality
Upratovanie	Milada Lacková (živnostníčka)

Tabuľka 7 Informačný systém obchodní partneri
(Zdroj: Vlastné spracovanie)

Informačný Systém Obchodných partnerov	
Dotknuté osoby	Kontaktné osoby právnických osôb
Kategória osobných údajov	*Uvedené v osobitnej tabuľke*
Účel	Objednanie tovaru a služieb (obojstranne)
	Platby a zmluvy
	Reklamácie
Príjemcovia	Firma, Zmluvní partneri
Sprostredkovatelia	Fakturačné oddelenie
Bezpečnostné opatrenia	Smernica o ochrane osobných údajov
Tretie strany	Nie
Právny základ	Spracúvanie nevyhnutné podľa osobitného predpisu alebo medzinárodnej zmluvy
	Obchodný zákonník č. 513/1991 Zb.
	Zákona č. 431/2002 Z. z. o účtovníctve

Sledované osobné údaje:

Tabuľka 8 Osobné údaje – obchodní partneri
(Zdroj: Vlastné spracovanie)

Názov osobného údaju	
Osobné údaje	● Meno ● Priezvisko ● Titul
Kompetenčné údaje	● Sídlo ● Pracovná pozícia
Kontaktné údaje	● Telefón ● Email

Zdroj dát

Dáta sú získané výhradne od obchodných partnerov pri uzatváraní zmluvy, alebo v priebehu plnenia predmetu tejto zmluvy.

Prístup k údajom

- **Obchod** má plný prístup k údajom, aby mohol v prípade formulačnej žiadosti vytvoriť zmluvu.
- **Marketing** má plný prístup k údajom. Vybavuje výstavy, spravuje sociálne siete, kampane a reklamy.
- **Riaditelia** majú plný prístup. Podpisujú zásadné zmluvy a udržujú chod spoločnosti.
- **Vedúci oddelení** majú plný prístup, vďaka ktorému vedia kontrolovať správnosť riešenia situácii svojich podriadených.

Vymazanie musí nastať

Podľa § 23 Právo na výmaz osobných údajov – podľa konkrétnych skutočností:

- Pri ukončení zmluvy
- Pri porušení zmluvy
- Po premlčaní doby archivácie potrebného dokumentu

1.2.4 Klienti

Klientom sa stáva každý zákazník, ktorý vytvorí objednávku služieb cez kontaktný formulár na oficiálnej stránke spoločnosti. Zákazník vypĺňa objednávku v e-shope, v ktorej vyjadruje súhlas s uchovávaním osobných údajov pre účely nevyhnutné na vytvorenie elektronickej zmluvy o službe alebo produkte. Tento súhlas vyjadruje zaškrtnutím prázdneho políčka „Súhlasím s obchodnými podmienkami.“ Na základe hypertextového odkazu si môže zákazník komplexne prečítať, čo do takýchto podmienok patrí.

Tabuľka 9 Spracovanie v IS – klienti
(Zdroj: Vlastné spracovanie)

Informačný Systém Klientov	
Dotknuté osoby	Fyzické osoby a kontaktné osoby právnických osôb
Spracovávané osobné údaje	*Uvedené v osobitnej tabuľke*
Účel	Predaj služieb, produktov
	Vytvorenie registračných údajov
	Platba a reklamácie
	Užívanie služieb
Príjemcovia **Sprostredkovatelia** **Bezpečnostné opatrenia**	Zamestnanci (L1,L2,L3,Marketing,Sales....)
	Účtovné oddelenie
	Smernica o ochrane osobných údajov
Tretie strany	Nie
Právny základ	Spracovanie na účely plnenia zmluvy
Bezpečnostné opatrenia	Obchodný zákonník č. 513/1991 Zb.
Tretie strany	Zákona č. 431/2002 Z. z. o účtovníctve

Sledované osobné údaje:

Tabuľka 10 Osobné údaje – klienti
(Zdroj: Vlastné spracovanie)

Názov osobného udajú	
Identifikačné údaje	● Meno ● Priezvisko ● Tituly ● Korešpondenčná adresa ● Fakturačná adresa ● Štátna príslušnosť
Kompetenčné údaje	● Názvy, doména, konkrétne služby
Osobné, kontaktné údaje	● Číslo ● E-mail

Zdroj údajov

Dáta, ktoré firma spracováva získava výhradne od zákazníkov prostredníctvom súhlasu so spracovaním osobných údajov pri objednávke.

Prístup k údajom

- **Technická podpora** má plný prístup ku klientom. Je s nimi v kontakte telefonicky, prípadne emailovo. Musia mať možnosť overiť zákazníka, nájsť ho v centrálnom registri a pomôcť klientovi so zakúpenými službami v systéme.
- **Obchod** má plný prístup k údajom, aby mohol vyhodnocovať aktuálne poskytované služby a ponúkať množstevné zľavy a produkty.
- **Marketing** má obmedzený prístup, ktorý neobsahuje citlivé údaje, avšak obsahuje typ zákazníka a jeho anonymný identifikátor, resp. Zoznamy zákazníkov podľa vybraných kategórii. Kategórie a zoznamy sú predmetmi kampaní.
- **Riaditelia** majú obmedzený prístup k zákazníkom.
- **Vedúci oddelení** majú plný prístup, vďaka ktorému vedia kontrolovať správnosť riešenia situácii svojich podriadených.

Vymazanie môže nastať:

Podľa § 23 Právo na výmaz osobných údajov – podľa konkrétnych skutočností:

- Po vypršaní lehoty pri archivácii údajov
- Po ukončení využívania služieb od spoločnosti
- Na žiadosť klienta*

*Pokiaľ klient žiadosť nepredloží, historické dáta sú naďalej uchovávané z dôvodu archivácie obchodných zmlúv.

1.2.5 Iné

Pod kategóriu "iné" sú zahrnutí zákazníci, ktorí sa zapoja do súťaží na výstavách, komentujú, prípadne kontaktujú spoločnosť prostredníctvom sociálnych sietí a inak vystavujú svoje osobné dáta. Táto kategória zahrňuje aj zákazníkov, ktorí navštevujú web, ale nevykonali žiadny nákup.

Tabuľka 11 – Informačný systém – Sociálne siete
(Zdroj: Vlastné spracovanie)

Informačný Systém Sociálne siete	
Dotknuté osoby	Fanúšikovia na sociálnych sieťach, návštevníci na výstavách a podobných udalostiach, Facebook, Google, Twitter
Spracovávané osobné údaje	Uvedené nižšie v osobných kategóriách
Účel	Propagácia tovarov a služieb potenciálnym a existujúcim zákazníkom, komunikácia s nimi
	Propagácia spoločnosti a firemnej kultúry ako zamestnávateľa
	Komunikácia navonok o aktivitách spoločnosti (šport, vzdelávanie a pod.)
Príjemca	Poskytovateľ telekomunikačných služieb
Sprostredkovatelia	Facebook, Google, Twitter
Bezpečnostné opatrenia	Smernica o ochrane osobných údajov
Tretie strany	Nie

Právny základ	Spracovanie na účely oprávneného záujmu

Tabuľka 11 Spracovanie IS – Webová stránka
(Zdroj: Vlastné spracovanie)

Informačný Systém Webová stránka*	
Dotknuté osoby	Návštevníci
Kategória osobných údajov	Identifikačné údaje
Účel	Optimalizácia obsahu webu
	Propagácia firmy a jej kultúry
	Prezentácia voľných pracovných miest
	Komunikácia navonok o spoločenských aktivitách spoločnosti (šport, charita, vzdelávanie a pod.)
Príjemcovia	Poskytovateľ telekomunikačných služieb
Sprostredkovatelia	Web-net s.r.o.
Bezpečnostné opatrenia	Smernica o ochrane osobných údajov
Tretie strany	Nie
Právny základ	Súhlas subjektu so spracovaním osobných údajov

Tabuľka 12 Osobné údaje – Webová stránka
(Zdroj: Vlastné spracovanie)

Názov osobného udajú	
Výstavy	● Meno ● Email
Facebook, Google, Linked IN, Twitter	● Meno a fotografia, prezývka
Webová stránka	● Ak je zákazník prihlásený – údaje zákazníka ● IP adresa ● Internetový prehliadač ● Operačný systém ● Dĺžka návštevy webu

*Dáta z webovej stránky samostatne neplnia definíciu osobných údajov, avšak zákazník môže iné osobné údaje v prípade potreby zadať. V takom prípade sa sledované

údaje z webovej stránky priradia k jeho zadaným osobným údajom. Do týchto údajov patria:

- Meno a priezvisko
- Kontaktný email

Prístup k údajom

- **Obchod a Marketing** má na starosti sekciu sociálnych sietí, odpisuje na správy, vykonáva a vybavuje objednávky a žiadosti.
- **Technická podpora** vidí osobné údaje návštevníka, akonáhle klikne na funkciu „chatu“ alebo vyplní formulár pre požiadavku.

Vymazanie musí nastať

Podľa § 23 Právo na výmaz osobných údajov – konkrétne:

- Koniec súťaže
- Zákazník odstráni komentár alebo príspevok na sociálnej sieti
- Sám zákazník požiada o vymazanie všetkých údajov zachytených o ňom ako subjekte

1.3 Informačné systémy

Vo firme funguje jedno hlavné úložisko dát, v ktorom sú osobné údaje uložené rovnakým spôsobom. Následne sa dáta distribuujú do konkrétnych informačných systémov pomocou vnútornej zabezpečenej siete firmy.

Tabuľka 13 Informačné systémy
(Zdroj: Vlastné spracovanie)

IS Klienti	INTRANET, Live Agent
IS obchodný partneri	Ekonix
IS Uchádzačov o zamestnanie	Vo forme emailu, alebo fyzickej formy.
IS Sociálne siete	Externé aplikácie

Intranet - Základný systém pre komplexné fungovanie firmy. Hlavné pracovisko, v ktorom sú vedené osobné údaje klientov. Pokrýva služby hostingu, profil zákazníka, fakturáciu a hlavné technické procesy v službách zákazníka (napr. logovanie aktivity).

Intranet zároveň pokrýva dochádzku zamestnanca (rozpis zmien, dovolenku, vyšetrenia a služobné cesty sú zaznamenané elektronicky v tomto systéme).

Live Agent – Externý systém prepojený s Intranetom, ktorý poskytuje komunikáciu so zákazníkmi formou chatu, telefonátov a emailovej komunikácie. Live Agent tvorí ID tiketov, ktoré sa následne priraďujú k zákazníkovi podľa intranetu a zamestnanec v prípade potreby môže preveriť problémy, ktoré sa u zákazníka v službe vyskytovali.

Ekonix – externá aplikácia pre mzdové a účtovné oddelenie. Systém spracováva pohľadávky a záväzky voči zamestnancom, obchodným partnerom a zákazníkom. Umožňuje fakturačnému oddeleniu tvoriť ostré faktúry a prípadné dobropisy.

Google Workspace - emailová komunikácia pre zamestnancov, ktorá zahrňuje schránku, kalendár a online meetingy, naviac je podporovaná na stolových aj mobilných zariadeniach.

1.4 Prístupy a bezpečnosť

Pre spracovanie a prístup k osobným údajom v spoločnosti Web-net s.r.o. boli definované nasledujúce skupiny subjektov. Keďže ide o vzťah interného prostredia k údajom z externého prostredia, boli určené typy oddelení, ktoré sa vo firme nachádzajú.

- Technická podpora
    - Vedúci oddelenia
    - L1 – Zákaznícka podpora
    - L2 – Technická podpora
    - L3 – Programátori
- Obchod
- Marketing
    - Vedúci oddelenia
    - Pracovníci
- Fakturačné oddelenie
- Riaditelia spoločnosti

Tabuľka 14 Prístupy zamestnancov k osobným údajom
(Zdroj: Vlastné spracovanie)

	Technické oddelenie	Obchod	Marketing	Fakturačné oddelenie	Riaditelia	Vedúci oddelení
OÚ zamestnancov						
OÚ zákazníkov						
Návšteníci webu OÚ						
OÚ dodávateľov						

Tabuľka 15 Vysvetlivky - Prístupy zamestnancov k osobným údajom
(Zdroj: Vlastné spracovanie)

	Prístup:	
Legenda		**Obmedzený**
		Úplný
		Žiadny

1.4.1 Online Prístup

Online prístup k dátam je uvedený v tabuľke č. 15. Systém funguje formou vlastného zabezpečeného intranet-u. Funguje len na vnútornej sieti. Zamestnanec vidí všetky informácie podľa priradeného prístupu. Zákazníka, služby, informácie o registrácii, údaje o výnosnosti, poskytnuté zľavy, históriu platieb, problémov a emailov vykonaných s daným zákazníkom.

Prideľovanie prístupových práv prebieha v dvoch krokoch:

1. Vytvorenie používateľského účtu zamestnanca
2. Pridelenie prístupových práv oprávnenej osobe

Oprávnenia a ďalšie činnosti navrhuje a vypracuje pracovník administrátor v spolupráci príslušným vedúcim oprávnenej osoby (zamestnanca). Rozsah oprávnení a zodpovedností sa realizuje na základe návrhu vedúceho zamestnanca oprávnenej osoby. Realizuje ju vedúci zamestnanec formou elektronickej alebo písomnej žiadosti, ktorá sa uchováva. Žiadosť sa odovzdá na ďalšie vybavenie oddeleniu informatiky, ktorý v zmysle svojich oprávnení pridelí oprávneným osobám prevádzkovateľa užívateľské práva. Oddelenie administrátorov o pridelení práv podľa smernice bezodkladne informuje príslušného vedúceho zamestnanca oprávnenej osoby. Oddelenie informatiky v

spolupráci s priamym nadriadeným oprávnenej osoby zaškolia a poučia oprávnenú osobu o práci a o manipulácii s dokumentmi obsahujúcimi osobné údaje a o zakázaných činnostiach pri manipulácii s osobnými údajmi. Po zaškolení a poučení oprávnená osoba podpisom na poučení potvrdí, že bola zaškolená a poučená.

Zamestnanec nesmie požívať pridelené prístupové práva na inú činnosť, ako je stanovená jeho pracovnou zmluvou, inou zmluvou, funkčným zaradením a náplňou práce. Zamestnanec nesmie poskytnúť svoje prístupové práva a identifikátor prístupu inej osobe. Prístupové práva tretích strán, ak to spracúvanie osobných údajov vyžaduje, prideľuje zodpovedná osoba v spolupráci s príslušným vlastníkom aktíva a za odbornej asistencie oddelenia informatiky. Prístupové práva sa prideľujú na dobu nevyhnutnú pre prístup do informačného systému.

1.4.2 Fyzická bezpečnosť osobných údajov

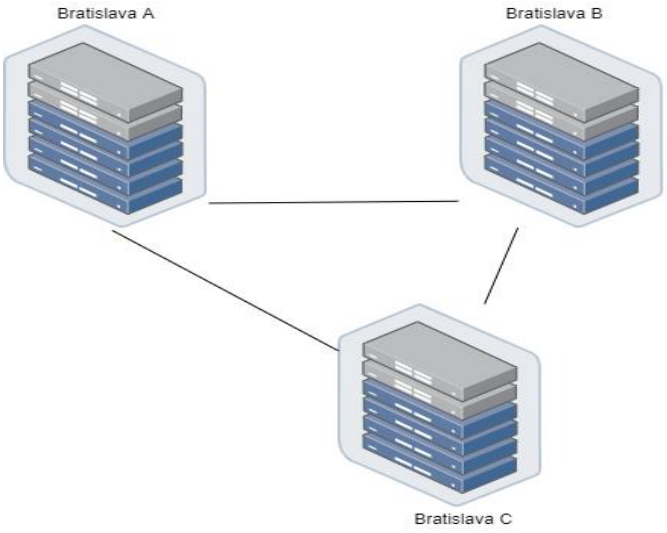
Budova, v ktorej sa spoločnosť nachádza je prenajímaná. Vlastník sa zaviazal energetickým certifikátom a splnením bezpečnostných a protipožiarnych predpisov.

Poloha budovy

Budova sa nachádza v odľahlej, kľudnej časti Trnavy. Okolie tvoria iné firmy, ktorá každá disponuje kamerovým systémom. Vstup do firmy je taktiež chránený kamerovým systémom. Záznam sa zachytáva nepretržite po dobu 2 týždňov. Pred vstupom je jasne viditeľné upozornenie o kamerovom snímaní objektu.

Umiestnenie serverov

Serverovňa v ktorej sa ukladajú osobné údaje sa nachádza priamo pod budovou. Táto serverovňa je spojená s dvoma ďalšími, nezávislými na sebe a redundantne zapojenými pomocou optických káblov vedených pod zemou. Pre bezpečné uchovanie dát sa využíva systém RAID.



Obrázok 1 Rozdelenie úložísk
(Zdroj: Vlastné spracovanie)

Fyzický Prístup

Fyzický prístup do **serverovní** je iba pre riaditeľov a zamestnancom povereným na výkon práce so servermi. Zamestnanec musí pri vstupe predložiť občiansky preukaz, kartičku povoľujúcu vstup a vrátnik ho na základe nej zapíše do systému evidencie.

1.4.3 Informačná bezpečnosť Osobných údajov

Firewall

Každý server má svoj vlastný firewall v operačnom systéme.

Pravidlá

Každý server má svoje firewall pravidlá a zároveň povolené iba konkrétne porty. Tieto porty a pravidlá závisia od typu a využitia servera.

IP adresy sú pevne určené tak, aby nikto s neoprávneným prístupom nemohol mať prístup.

Heslá

Primárne zamestnanci využívajú SSH kľúče. V prípade hesiel klasických hesiel sú určené pravidlá vytvárania hesla.

Zálohovanie

Prebieha každý deň medzi 22:00 – 23:00. Denné zálohy sa robia po dobu mesiaca, následne sa robia mesačné zálohy vo forme „snapshotov“, najviac však pol roka. Snapshoty sa ukladajú na oddelené zálohovacie servery v inej geolokácii ako je samostatný server s ostrými dátami.

Firma nedisponuje žiadnou internou smernicou, ktorá by pokrývala situácie v prípade ohrozenia dát, pre obnovu a postupov zálohovania dát. Tieto informácie sa predávajú iba ústnou formou.

Kryptovanie

V súčasnosti firma nevyužíva žiadne kryptovanie na žiadnej komunikačnej sfére.

VPN

Pokiaľ zamestnanec nie je fyzicky pripojený na sieť, musí sa overiť formou VPN, ktorá pomocou prihlasovacích údajov zamestnancovi dovolí pripojiť sa do vnútornej infraštruktúry.

Antivírusová ochrana

Na antivírusovú ochranu pracovných staníc je primárne určený softvérový systém, ktorý je automaticky pravidelne aktualizovaný. Používatelia majú zakázané odinštalovanie, zablokovanie alebo zmenu konfigurácie antivírusovej ochrany. Za inštaláciu, aktualizáciu, zmeny konfigurácie a previerky antivírusových systémov, ako aj za bezodkladné riešenie problémov spojených s existenciou vírusov, zodpovedá oddelenie informatiky. Pokiaľ má zamestnanec podozrenie, že jeho antivírusový systém nepracuje správne, musí informovať oddelenie zákazníckej podpory. Zamestnanci majú zakázané používať pracovné stanice, na ktorých antivírusový systém nepracuje, alebo nepracuje správne. Prenosné médium musí byť pred použitím skontrolované na prítomnosť vírusov rezidentnou antivirusovou ochranou, nachádzajúcou sa na každej pracovnej stanici.

1.5 Organizačné opatrenia

1.5.1 DPO - poverená osoba

Právne predpisy neukladajú povinnosť mať takúto osobu vo firme, nakoľko nespĺňa ani jedno z kritérií pre menovanie zodpovednej osoby. Firma ňou teda nedisponuje.

1.5.2 Smernica

Firma disponuje aktuálnou smernicou o ochrane osobných údajov, ktorú vypracovala externá firma na objednávku v roku 2018. Obsahuje:

- Účel a vymedzenie zodpovednosti
- Zásady spracúvania osobných údajov a právny základ ich spracúvania
- Práva a povinnosti(dotknutej osoby aj oprávnenej osoby)
- Technické a organizačné opatrenia
- Organizačné opatrenia – personálne, zoznamy aktivít, likvidácia, bezpečnostné incidenty
- Záverečné ustanovenia
- Prílohy zmlúv

1.5.3 Firemné Školenia

Firemné školenia sú pre zamestnancov v každom oddelení, líšia sa poľa potrieb konkrétneho oddelenia. Školenia ktoré zasahujú do práce s osobnými údajmi sa rozdeľujú nasledovne:

- **Školenia o ochrane osobných údajov –** pre každého novoprijatého zamestnanca a v prípade potreby re-edukácii ostatných zamestnancov. Neopakujú sa pravidelne, nakoľko to nevyžaduje zákon a vykonáva ich externý špecialista na ochranu OÚ.
- **Interné školenia zamestnancov o výkone práce** – podľa potrieb konkrétnych oddelení, prebiehajú buď osobitne alebo celofiremne.

- **Bezpečnostné školenia BOZP** – pre každého novoprijatého zamestnanca pri nástupe do výkonu práce. Následne preškolenia prebiehajú každých 12 mesiacov externým špecialistom.

1.5.4 Dokumenty, ich skartácia a likvidácia

Archív papierových dokumentov má v kompetencii pracovník fakturačného oddelenia. Tieto údaje sú uložené v priestore open office, vo vyčlenenom rohu miestnosti pre fakturačné oddelenie. Firma prešla v roku 2020 na čisto online vedený IS zmlúv, avšak z historického hľadiska drží dokumenty aj v papierovej forme, do dňa uplynutia nutnej lehoty. Táto časť pokrýva pracovné zmluvy zo zamestnancami, obchodné zmluvy s partnermi a iné administratívne dokumenty. Dokumenty sú uložené podľa nadobudnutia a roztriedené podľa nutnej archivačnej lehoty. **Skartácia dokumentov** prebieha podľa dôležitosti. Prebieha raz ročne povereným zamestnancom.

Firma nedisponuje smernicou o archivácii a skartácii dokumentov.

1.5.5 Likvidácia osobných údajov a dátových nosičov

Pri vyraďovaní a likvidácií softvéru, hardvéru a médií, je zamestnanec povinný zaistiť bezpečnú likvidáciu údajov na vyraďovaných zariadeniach a médiách. Rovnako sa postupuje aj v prípade preradenia pamäťových médií na iné využitie, ako na spracovanie (uloženie) osobných údajov alebo iných citlivých informácií, resp. preradenie zariadenia inému zamestnancovi. Nepotrebné súbory s osobnými údajmi na médiách zamestnanec bezodkladne vymaže. Nepotrebné a nepoužiteľné médiá zamestnanec fyzicky zlikviduje, v prípade potreby v súčinnosti s oddelením IT. Zamestnanec, ktorý zodpovedá za vyradenie média, zabezpečí jeho fyzickú likvidáciu tak, aby údaje aj nosič boli nevratne znehodnotené. Fyzicky zlikvidované musia byť predovšetkým tie médiá, ktorých obsah sa nedá natrvalo vymazať. Tieto informácie sú zakotvené v smernici o ochrane osobných údajov.

1.6 Požiadavky zadávateľa

Klient, spoločnosť Web-net s.r.o. sa nezaoberá právnymi záležitosťami a preto požiadala o vypracovanie pre:

- Analýzu legislatívy v oblasti ochrany osobných údajov
- Kontrolu korektnosti prístupov k osobným údajov
- Overenie mechanizmu spracovania osobných údajov
- Korektúru internej smernice podľa požiadaviek štátu
- Návrh a úprava doposiaľ nadobudnutých dokumentov a korektný výstup v rámci transparentnosti a úplnosti podľa nariadenia a zákona č. 18/2018 Z. z. o ochrane osobných údajov
- Vytvorenie smerníc pokrývajúcich nezabezpečené miesta v analýze

Hlavná požiadavka je, aby táto práca slúžila ako základ metodiky pre uplatnenie GDPR, následnú integráciu do spoločnosti a zaistenie súladu. Zoštylizovať systém tak, aby bol dostatočne modulárny a pripravený pre budúce zmeny v zákone.

1.7 Zhrnutie analýzy

Firma pôsobí na trhu už od roku 2001, čo znamená, že postupom času sa infraštruktúra tvorila, dopĺňala a formovala podľa potrieb zákonov a smerníc. Po podrobnej analýze je možné zachytiť niekoľko nezrovnalostí v spracovaní osobných údajov. Tieto nezrovnalosti nie sú deštruktívne, avšak môžu spôsobiť niekoľko rozporov, prípadne nechcených právnych konaní. Body pre úpravu sú:

Tabuľka 16 Hrozby nájdené v spoločnosti
(Zdroj: Vlastné spracovanie)

Chyby nájdene v analýze prostredia	
Uchádzač o zamestnanie	Ak uchádzač pošle email s životopisom, po ukončení konania sa ďalej nepreveruje, či poverený zamestnanec email odstránil.
Viditeľné osobné údaje pri chatovaní	Zákazník pri začatí chatovej komunikácie neodsúhlasí, že údaje spomenuté v chate sú dobrovoľne poskytnuté.

Prístupy	Prístupy k osobným údajom má priveľa zamestnancov.
Kryptovanie	Nenastavené žiadne kryptovanie
Zálohovanie	Nedostatočné zálohovanie, zálohy sú vedené krátke časové obdobie.
Zodpovedná osoba	Spoločnosť nemá určenú zodpovednú osobu na dohľad spracovania GDPR ! nie DPO
Archivované zmluvy	Zmluvy s obchodnými partnermi neprešli aktualizáciou a nie sú vedené podľa nového GDPR.
Pravidlá emailovej komunikácie	Nie sú definované, sú len ústne podávané
Cookies	Pri súhlase s cookies sa zákazník nemôže prekliknúť na podmienky
Budúce konanie vo firme	Chýbajú opatrenia, ktoré by zaisťovali budúci súlad s GDPR
Bezpečnosť prevádzky	Pri komunikácii nie sú vytvorené jednotné šablóny, štandardizované jednotky ktoré by plnili funkciu korektnosti pri pracovaní s OÚ.
Dokumenty	Tlačené dokumenty sú voľne archivované, nie sú pravidelne odstraňované po ukončení lehoty.
Dokumenty	Nie sú uzamknuté, sú voľne dostupné v Office.
Hardware	Chýba sieťový firewall.
Smernica	Chýba interná smernica pre zamestnancov.

Tabuľka 17 kontrola Prístupov zamestnancov k osobným údajom
(Zdroj: Vlastné spracovanie)

	Technické oddelenie	Obchod	Marketing	Fakturačné oddelenie	Riaditelia	Vedúci oddelení
OÚ zamestnancov						
OÚ zákazníkov						
návštevníci webu OÚ						
OÚ dodávateľov						

Tabuľka 18 Legenda vhodnosti
(Zdroj: Vlastné spracovanie)

	Vhodnosť	
Legenda		V poriadku
		Preveriť
		Zlá

2 TEORETICKÉ VÝCHODISKA PRÁCE

2.1 Vymedzenie základných pojmov

Nariadenie GDPR

Nariadenie Európskeho parlamentu a Rady EÚ 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane osobných údajov).

Smernica o ochrane osobných údajov

Smernica európskeho parlamentu a rady (EÚ) 2016/680 z 27. Apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov a o zrušení rámcového rozhodnutia rady 2008/977/svv.

Zákon

Zákon č. 18/2018 Z. z. o ochrane osobných údajov a zmene a doplnení niektorých zákonov.

Osobné údaje

„Osobné údaje sú akékoľvek informácie týkajúce sa identifikovanej alebo neidentifikovateľnej fyzickej osoby. identifikovateľná fyzická osoba je osoba, ktorú možno identifikovať priamo alebo nepriamo, najmä odkazom na identifikátor, ako je meno, identifikačné číslo, lokalizačné údaje, online identifikátor, alebo odkazom na jeden či viaceré prvky, ktoré sú špecifické pre fyzickú, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu tejto fyzickej osoby.“[2]

Spracúvanie

„Spracúvanie je operácia alebo súbor operácií s osobnými údajmi alebo súbormi osobných údajov, napríklad získavanie, zaznamenávanie, usporadúvanie, štruktúrované, uchovávanie, prepracovanie alebo zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo poskytovanie iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie alebo likvidácia, bez ohľadu na to, či sa vykonávajú automatizovanými alebo neautomatizovanými prostriedkami“ [2]

Informačný systém

Informačný systém je akýkoľvek usporiadaný súbor osobných údajov, ktoré sú prístupné podľa určených kritérií, bez ohľadu na to, či ide o systém centralizovaný, decentralizovaný alebo distribuovaný na funkčnom alebo geografickom základe[4]

Prevádzkovateľ

„Prevádzkovateľ je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý sám alebo spoločne s inými určí účely a prostriedky spracúvania osobných údajov; v prípade, že sa účely a prostriedky tohto spracúvania stanovujú v práve Únie alebo v práve členského štátu, možno prevádzkovateľa alebo konkrétne kritériá na jeho určenie určiť v práve Únie alebo v práve členského štátu“ [2]

Sprostredkovateľ

„Sprostredkovateľ je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý spracúva osobné údaje v mene prevádzkovateľa“ [2]

Príjemca

„Príjemca je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorému sa osobné údaje poskytujú bez ohľadu na to, či je treťou stranou. Orgány verejnej moci, ktoré môžu prijať osobné údaje v rámci konkrétneho zisťovania v súlade s právom Únie alebo právom členského štátu, sa však nepovažujú za príjemcov; spracúvanie uvedených údajov uvedenými orgánmi verejnej moci sa uskutočňuje v súlade s uplatniteľnými pravidlami ochrany údajov v závislosti od účelov spracúvania.“ [2]

Tretia strana

„Treťou stranou je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt než dotknutá osoba, prevádzkovateľ, sprostredkovateľ a osoby, ktoré sú na základe priameho poverenia prevádzkovateľa alebo sprostredkovateľa poverení spracúvaním osobných údajov.“ [2]

Chat

Online komunikácia tvorená formou rýchlych správ. Komunikanti odpovedajú v priebehu niekoľkých sekúnd, na rozdiel od emailovej komunikácie. [5]

Hosting

Virtuálny priestor, ktorý poskytuje spoločnosť vo forme prenájmu na ich serverových úložiskách. [6]

E-shop

Obchod prevádzkovaný výlučne online formou, na hostingovom priestore.

Snapshot

Výpočtový výraz, ktorý označuje kópiu vytvorenú z diskovej jednotky v konkrétnom časovom okamihu. Snímky sú užitočné na zálohovanie údajov v rôznych intervaloch, čo umožňuje obnovenie informácií z rôznych časových období. [7]

Server

Server je počítač, ktorý poskytuje údaje iným počítačom. Môže slúžiť na prenos údajov do systémov v lokálnej sieti (LAN) alebo rozsiahlej sieti (WAN) cez internet. [8]

Hacker

Niekto, kto môže získať neoprávnený prístup k iným počítačom. Hacker môže „hacknúť" svoju cestu cez úrovne zabezpečenia počítačového systému alebo siete. [9]

RAID

Znamená „redundantné pole nezávislých diskov". RAID je metóda ukladania údajov na viac pevných diskov. Ak sú disky usporiadané v konfigurácii RAID, počítač ich všetky vidí ako jeden veľký disk. Technika spočíva v rozdeľovaní uložených údajov medzi dostupné disky. [10]

Zodpovedná osoba DPO

„Zodpovednou osobou je oprávnená osoba, ktorá zabezpečuje dohľad nad ochranou osobných údajov pri spracúvaní osobných údajov u prevádzkovateľa alebo sprostredkovateľa." [11]

Cookies

Súbory cookie sú malé dátové súbory, ktoré sa odosielajú zo servera webovej stránky do vášho webového prehliadača, odkiaľ sa ukladajú do vášho zariadenia. [12]

SSL

SSL šifruje prenášané údaje cez http. Údaje dokáže rozpoznať iba počítač používateľa a zabezpečený server. Protokol SSL uchováva informácie medzi zákazníkom a obchodníkom, ktorému ich poskytuje. Pri návšteve webovej adresy začínajúcej na

„https“, znak „s“ za „http“ označuje, že web je bezpečný. Webové stránky používajú certifikáty SSL na overenie ich pravosti. [13]

2.2 Informácie, dáta

Skúmanie informácií naráža na okamžité ťažkosti, nakoľko pojem informácia je vhodný iba vo vzťahu k niekomu informovanému, z dôvodu nevedomosti a neistoty, je ironické, že samotný pojem informácia je nejednoznačný a používa sa rôznymi spôsobmi.

Zoči-voči rozmanitosti významov môžeme zaujať prinajmenšom pragmatický prístup. Ak možno identifikovať, triediť, charakterizovať slovo informácia, tak pomocou tohto prístupu sa identifikujú tri hlavné použitia slova:

I. **Informácie ako proces:** To, čo niekto vie, sa zmení, keď je informovaný. V tomto zmysle sú informácie činom informovania komunikáciou poznatkov alebo„ správ “o nejakej skutočnosti alebo udalosti.

2. **Informácie ako vedomosti:** Informácie sa používajú na označenie toho, čo sa prenáša v procese informovania: oznamované poznatky sa týkajú určitej konkrétnej skutočnosti, predmetu alebo udalosti; inak povedané dáta, ktoré nesú hodnotu.

3. **Informácie ako vec:** Objekty, ako sú údaje a dokumenty sa označujú informácie, pretože sa považujú za informatívne - za vedomosti alebo komunikačné informácie.

Kľúčovou charakteristikou je, že je nehmotná. Jej základnou jednotkou sú dáta. Dáta je potrebné spracovať a následne z nich je možné vyvodiť informácie.[14]

2.3 Osobné údaje a ich rozdelenie

Osobné údaje sú akékoľvek informácie, ktoré sa týkajú identifikovaného jednotlivca. OÚ tvoria aj rôzne iné informácie, ktoré spoločne môžu viesť k identifikácii konkrétnej osoby. Rovnako to platí pre osobné údaje, ktoré boli de-identifikované, šifrované alebo pseudonymizované, a je možné ich použiť na opätovnú identifikáciu osoby. Aby boli údaje skutočne anonymizované, musí byť anonymizácia nezvratná. [15]

GDPR významne rozširuje definíciu osobných údajov tak, aby zahŕňala všetky informácie, ktoré je možné spojiť so známou osobou. Príklady zahŕňajú históriu prehliadača a aktivitu na sociálnych sieťach. Prijíma tiež osobitné ustanovenia pre

informácie týkajúce sa fyzického a duševného zdravia jednotlivca, ako sú genetické a biometrické údaje. [15]

Osobné údaje je možné rozdeliť do niekoľko kategórii:

Obrázok 2 Rozdelenie osobných údajov

(Zdroj: Vlastné spracovanie podľa [16])

2.3.1 Bežné osobné údaje

Niektoré zo sprocesovaných dát môžu byť menej citlivé ako tie ostatné. Do bežných údajov sa radia údaje, vďaka ktorým je možno konkrétnu osobu identifikovať. Neexistuje definitívny zoznam toho, čo sú alebo nie sú osobné údaje, takže všetko závisí od správnej interpretácie definície GDPR. [15]

Tabuľka 19 Spracovanie bežných údajov
(Zdroj: Vlastné spracovanie)

Názov OÚ	Popis údajov	Právny pôvod*
Identifikačné údaje	Slúžia predovšetkým k určeniu najosobnejších dát ktoré primárne identifikujú osobu.	*a) dotknutá osoba vyjadrila súhlas so spracovaním svojich osobných údajov na jeden alebo viaceré konkrétne účely;* *b) spracúvanie je nevyhnutné na plnenie zmluvy, ktorej zmluvnou stranou je dotknutá osoba, alebo aby sa na základe žiadosti dotknutej osoby vykonali opatrenia pred uzatvorením zmluvy;* *c) spracúvanie je nevyhnutné na splnenie zákonnej povinnosti prevádzkovateľa;* *d) spracúvanie je nevyhnutné, aby sa chránili životne dôležité záujmy dotknutej osoby alebo inej fyzickej osoby;* *e) spracúvanie je nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi;* *f) spracúvanie je nevyhnutné na účely oprávnených záujmov, ktoré sleduje prevádzkovateľ alebo tretia strana, s výnimkou prípadov, keď nad takýmito záujmami prevažujú záujmy alebo základné práva a slobody dotknutej osoby, ktoré si vyžadujú ochranu osobných údajov, najmä ak je dotknutou osobu dieťa*. [17]
Sociálne	Vymedzujú všeobecný denný život konkrétnej osoby, jeho vplyv v spoločnosti.	
Finančné	Opisujú pohyb peňazí a identifikujú osobu z finančného hľadiska.	
Kontaktné údaje	Ako osobu môžeme vyhľadať/kontaktovať - napr. Email, číslo, adresa bydliska.	

*Právny pôvod je vedený podľa zákonnosti v čl.6 „ EÚ všeobecne nariadenie o ochrane osobných , určuje, kedy sa takéto údaje môžu spracovávať

2.3.2 Citlivé údaje

V tejto kategórii sa nachádzajú dáta, ktoré identifikujú osobu z hľadiska náboženského, procesného alebo osobného – každodenného života. Tieto údaje sú zvlášť

dôležité a musia byť špeciálne chránené, nakoľko ich krádežou by mohlo prísť k nebezpečným protiprávnym činnostiam.[15]

Tabuľka 20 Spracovanie osobných údajov
(Zdroj: Vlastné spracovanie)

Názov OÚ	Popis údajov	Právny pôvod*
Národnostné	Vypovedá o etnicite, národnostnom a rasovom pôvode.	*a) dotknutá osoba vyjadrila výslovný súhlas so spracúvaním týchto osobných údajov na jeden alebo viacero určených účelov, s výnimkou prípadov, keď sa v práve Únie alebo v práve členského štátu stanovuje, že zákaz uvedený v odseku 1 nemôže dotknutá osoba zrušiť;* *b) spracúvanie je nevyhnutné na účely plnenia povinností a výkonu osobitných práv prevádzkovateľa alebo dotknutej osoby v oblasti pracovného práva a práva sociálneho zabezpečenia a sociálnej ochrany, pokiaľ je to povolené právom Únie alebo právom členského štátu alebo kolektívnou zmluvou podľa práva členského štátu poskytujúcimi primerané záruky ochrany základných práv a záujmov dotknutej osoby; [17]*
Audiovizuálne	Pokrývajú všetky fotografie, video a audio nahrávky danej osoby.	
Náboženské a politické	Zahŕňa presvedčenie, vierovyznanie a filozofický smer.	
Trestnoprávne	Pokrýva odsúdenie, trestné činy a celkovú trestnú históriu osoby.	
Zdravotné údaje	Obsahuje zdravotný stav , sexuálne preferencie a genetické údaje osoby.	

*Právny pôvod je vedený podľa zákonnosti v čl.6 „ EÚ všeobecne nariadenie o ochrane osobných údajov. Určuje, kedy sa takéto údaje môžu spracovávať.

2.4 GDPR

Všeobecné nariadenie o ochrane osobných údajov alebo GDPR je nové nariadenie Európskej únie, ktoré nahrádza, ruší smernicu 95/46/ES a upravuje predošlý zákon o ochrane osobných údajov. Vyplýva z rešpektovania súkromia, sociálneho a iného života konkrétnej osoby a tým pádom značne obmedzuje sledovanie týchto údajov.

Základným kameňom GDPR je súhlas. Súhlas bol potrebný aj pred úpravou, ale získať ho bolo oveľa jednoduchšie. V súvislosti s novými predpismi už nie je získanie súhlasu isté. GDPR jasne hovorí, že pokiaľ nejde o oprávnený záujem, prinútenie

klientov, aby povedali áno, je potrebné urobiť výslovným spôsobom, jednoduchým jazykom a objasniť dôvody, pre ktoré sa vyžaduje súhlas. Používateľ musí presne vedieť, na aký účel a kto bude používať jeho osobné údaje. Uplatňovanie najprísnejších výkladov s využitím osobných údajov občana EÚ si vyžaduje, aby bol takýto súhlas slobodný, konkrétny, informovaný a jednoznačný. Vyžaduje si to pozitívny prejav súhlasu - nemožno to vyvodiť z ticha, vopred začiarknutých políčok alebo nečinnosti. [15]

Európska komisia prišla v roku 2012 s návrhom zjednotiť zákon o ochrane OÚ, ktorý doposiaľ pokrývala len všeobecné nariadene o ochrane OÚ v smernici 95/46/ES. V smernici 95/46/ES boli zásady zamerané len na ochranu základných práv a slobôd pri spracovaní osobných údajov. V novej smernici GDPR sa časť zaoberá ochranou OÚ pri spracúvaní osobných údajov, zároveň však aj ich voľným pohybom. Táto nová smernica bola schválená v roku 2016 a nabrala účinnosť 25.5.2018. Dotýka sa všetkých európskych, alebo mimoeurópskych subjektov pôsobiacich na európskom trhu, ktoré spracúvajú osobné údaje v rámci svojej pôsobnosti. To znamená, že do tohto dátumu musia všetky firmy popísané vyššie vytvoriť jednotný systém, ktorý bude spĺňať všetky povinnosti nariadenia o GDPR. [18]

Zmeny v smernici GDPR v porovnaní s 95/46/ES

1. **Právny nástroj a jeho forma**

   Došlo k zjednoteniu právneho nástroja tak, aby bol rovnako aplikovateľný v členských štátoch, ďalej k zjednoteniu orgánov dozoru pri vynucovaní povinností, ktoré boli stanovené v GDPR. Tomu pomôžu konkrétne právne inštitúty, ako EDPD.

2. **Širšia pôsobnosť pravidiel**

   GDPR sa aplikovalo aj na tretie krajiny (mimo EÚ), ktoré pôsobia / podnikajú v EÚ alebo kontrolujú údaje zákazníkov z EÚ.

3. **Jediné kontaktné miesto**

   Vytvorenie jedného právneho inštitútu, ktorý zjednodušil subjektom kontakt pri riešení problémov v dodržiavaní smernice GDPR. Stojí na dvoch bodoch: Určenie hlavnej prevádzkarne v EÚ a určenie hl. dozorného orgánu

4. **Konkretizácia osobných údajov**

   Za osobné údaje sú považované aj identifikátory osôb v online sfére (cookies, adresa IP, iné el. identifikátory).

5. **Posilnenie princípu zodpovednosti** za osobné údaje. [18]

Pre koho platí smernica GDPR

„GDPR platí pre každého, kto zhromažďuje a spracováva osobné údaje Európanov, vrátane spoločností a inštitúcií mimo EÚ, ktoré pôsobia na európskom trhu. Nariadenie je platné pre firmy, inštitúcie, jednotlivcov – zamestnancov, zákazníkov, klientov aj dodávateľov naprieč všetkými odvetviami. Týka sa aj tých, ktorí analyzujú chovanie užívateľov webov a aplikácií. To môžu byť Online obchody, banky, poisťovne, sociálne a zdravotné inštitúcie, štátne firmy a oblasti verejného práva, zdravotníctvo.“ [19]

2.4.1 História

↓ Všeobecná deklarácia ľudských práv

- 10. december 1948
- prijatá OSN, popisuje kmeňové ľudské práva
- Táto deklarácia slúži len ako vzor pre záväzné zákony a právne normy. Nemá funkčnosť právneho dokumentu. [20]

↓ Dohovor o ochrane ľudských práv a slobôd

- 4. novembra 1950
- Najzakladanejší a najdôležitejší dokument na európskom kontinente. Zahŕňa najdôležitejšie práva pre človeka a obsahuje príležitosti, ktoré umožňujú jedincom brániť sa proti štátu v prípade , že im tieto práva neposkytuje. [21]

↓ Smernica 95/46 /ES

- 24.oktober 1995
- Prijatá prvá európska smernica o ochrane osobných údajov
- Popisuje ochranu fyzických osôb, spracovanie OÚ a voľný pohyb týchto údajov[22]

↓ Všeobecné nariadenie o ochrane osobných údajov

- 27.apríl 2016
- **Nariadenie Európskeho parlamentu a Rady (EÚ)** 2016/679 z 27. apríla 2016 o ochrane fyzických osôb v súvislosti so spracovaním osobných údajov a o voľnom pohybe týchto údajov, ktorým sa zrušuje smernica 95/46 / ES
- GDPR prináša právo dotknutej osoby na prenosnosť osobných údajov alebo zavedenie inštitútu poverenej osoby pre ochranu osobných údajov. GDPR kladie systematicky dôraz na vymáhateľnosť práva osôb a povinností správcov. [23]

↓ Platnosť GDPR

- 25.máj 2018
- **Od tohto dňa platí všeobecné nariadenie o ochrane údajov**. Niektoré organizácie, napríklad tie, ktorých hlavnou činnosťou je pravidelné a systematické monitorovanie osobných alebo citlivých údajov vo veľkom rozsahu, ako aj organizácie vo verejnom sektore, budú musieť vymenovať úradníka pre ochranu údajov, ktorý zabezpečí dodržiavanie GDPR. [22]

2.4.2 Správca a spracovateľ

Správca / prevádzkovateľ je kľúčovým rozhodovacím orgánom. Má celkovú kontrolu, kontrolu nad dôvodmi a účelmi zhromažďovania údajov a nad prostriedkami a metódou spracovania údajov. Je povinný prijať a zároveň zabezpečiť technické a organizačne opatrenia pre spracúvanie osobných údajov v súlade so zákonom. Tieto opatrenia musí pravidelne aktualizované. Je povinný pravidelne preverovať účely a trvanie spracovania OÚ a v prípade jeho splnenia bezodkladne zabezpečiť výmaz OÚ. [24]

Povinnosti správcu:

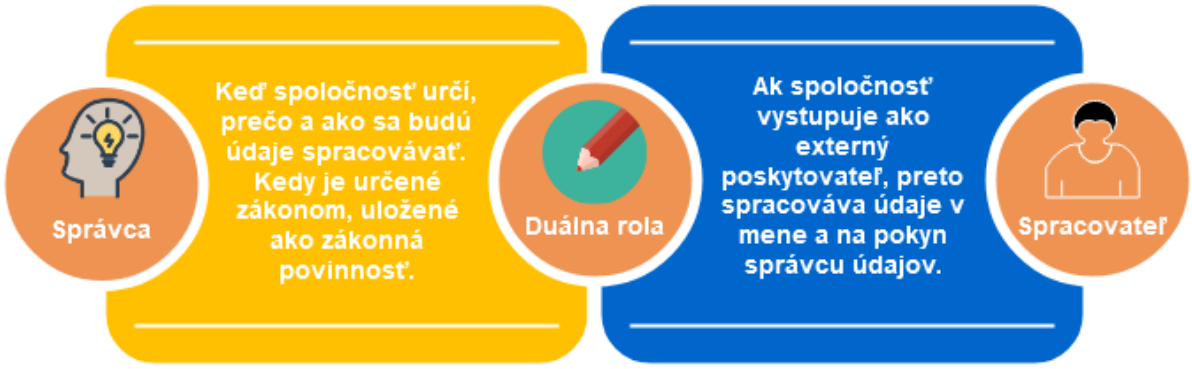
- Stanoviť účel
- Získať súhlas objektov
- Oznamovacia povinnosť [25]

Povinnosti správcu pri spracovaní:

- Spracovávať pravdivé a presné OÚ
- Zhromažďovať údaje Odpovedajúce účelu
- Spracovávať OÚ v súlade s pôvodným účelom
- Nezdružovať OÚ
- Prijať bezpečnostné opatrenia
- Ďalšie povinnosti pri spracovaní OÚ [25]

Spracovateľ údajov koná v mene prevádzkovateľa. Fungujú iba podľa pokynov od správcov. Jednotliví užívatelia môžu požadovať náhradu škody a náhradu škody voči procesorom aj kontrolórom. Tento vzťah je nutné predložiť záväznou dohodou. Tak aby boli pokryté náležitosti z článku 28. [25]

Existujú firmy, ktoré vystupujú aj v roli spracovateľa aj správcu:



Obrázok 3 Správca a spracovateľ
(Zdroj: Vlastné spracovanie podľa[26])

2.4.4 Dotknuté osoby

Za takúto osobu sa považuje každá fyzická osoba, ktorá je vlastníkom preberaných osobných údajov. Dotknutou osobou nemôže byť právnická, ani žiadna iná osoba – podnikateľ, alebo družstvo. Dotknutou osobou je výhradne jednotlivec ako fyzická osoba. [27]

2.5 Zákonné úpravy Slovenskej Republiky

Ochrana OÚ na úrovni práva Európskeho sa dotýka aj Slovenskej Republiky, nakoľko je nutná si plniť svoje záväzky ako členský štát Európskej únie. Transponovanie smernice a zosúladenie vnútroštátneho poriadku sa stalo nutnosťou pre splnenie Zmluvy o Európskej únii a Zmluvy o fungovaní Európskej Únii. To predchádzalo vytvoreniu Zákona o ochrane osobných údajov, ktorý transponuje Smernicu Európskeho parlamentu a rady (EÚ) č. 2016/680 z 27. apríla 2016 o ochrane fyzických osôb. [37]

Prehľad procesov transpozície smernice do podmienok SR

Návrh zákona je delený do niekoľko bodov. Prvý, druhý a tretí bod zákona je takmer identický so smernicou GDPR. Iba preklápajú nariadenie. Štvrtý bod zákona opisuje ochranu OÚ v situáciách odhaľovania trestnej činnosti a jej predchádzaniu. Piata časť opisuje osobitné situácie. Tento bod sa značne líši od smernice GDPR - opisuje situácie pri sprístupňovaní a zverejňovaní osobných údajov. Posledné dva body upravujú aspekty procesov a prechodných ustanovení. Tieto body ponecháva GDPR čisto k regulácii štátom. [38]

Nový návrh zákona o ochrane osobných údajov			
1. bod	Základné ustanovenia (vecná a územná pôsobnosť)	• Oblasti, ktoré nie sú pokryté právom EÚ a na spoločnú bezpečnostnú a zahraničnú politiku	 **Irelevantná pre väčšinu spracovateľských operácii v súkromnom sektore a verejnej správy.**
2. bod	Vymedzenie základných pojmov	• Oblasti, ktoré nie sú pokryté právom EÚ a na spoločnú bezpečnostnú a zahraničnú politiku	
3. bod	Pravidlá spracúvania OÚ	• Oblasti, ktoré nie sú pokryté právom EÚ a na spoločnú bezpečnostnú a zahraničnú politiku	
4. bod	Transpozícia policajnej smernice 2016/680/EÚ do právneho poriadku SR	• Orgány pôsobiace v oblasti predchádzania a odhaľovania trestnej činnosti	
5., 6., 7. bod zákona	Implementácia časti GDPR na základe splnomocňujúcich ustanovení	• Upravuje aspekty, ktoré GDPR ukladá alebo umožňuje členským štátom upraviť v medziach právneho rámca nariadenia	 **Aplikovaná v súkromnom aj vo verejnom sektore.**

Obrázok 4 Rozdelenie nového zákona o ochrane OÚ
(Zdroj: Spracovanie podľa [38])

Smernica GDPR v niektorých sektoroch umožnila vytvoriť osobitné pravidlá dodržiavania nariadenia a ich sankciu v prípade porušenia. V zákone prišlo k prijatiu vnútroštátnej úpravy nariadení vo viacerých paragrafoch. V § 78 vymedzila osobitné situácie pre spracúvanie OÚ, v § 79 povinnosť zachovania mlčanlivosti, v §105 a §106 vytýčila poriadkové pokuty.

Podľa paragrafu §78 sú nasledovné osobitné situácie pre spracúvanie:

- V prípade umeleckých, akademických, alebo literárnych účelov a účelov masovej komunikácie verejnosti nie je potrebný súhlas dotknutej osoby.
- Prevádzkovateľ ako zamestnávateľ môže zverejniť údaje dotknutej osoby v rozsahu meno a priezvisko, pozíciu, tel. číslo, email a miesto výkonu práce.

- Pri spracovaní OÚ možno využiť rodné číslo ako identifikátor v prípade daného účelu spracovania. Zakazuje sa však zverejňovať rodné číslo.
- V prípade zosnulej osoby, jej súhlas môže vydať blízka osoba iba ak žiadna iná blízka osoba písomne nevyslovila súhlas.
- V prípade účelu archivácie, vedeckého, štatistického, alebo historického výskumu ide o tzv „privilegované účely“ ktoré patria pod výnimku zo zásady obmedzenia účelu. Prevádzkovateľ však musí prijať primerané opatrenia. [37]

Paragraf §79 stanovuje povinnosť **o mlčanlivosti** prevádzkovateľovi a sprostredkovateľovi. Obdobne mlčanlivosť platí aj pre zamestnancov, ktorý prídu do styku s OÚ vo výkone práce aj po skončení pracovného vzťahu. Výnimkou povinnosti mlčania je nevyhnutné plnenie úlohy súdu alebo orgánov činných v trestnom konaní. [37]

Paragraf §105 upravuje **poriadkové pokuty.** V prípade osoby, ktorá nie je prevádzkovateľom, ani sprostredkovateľom do výšky 2 000 € za nesúčinnosť pri danom výkone dozoru, alebo prevádzkovateľovi a sprostredkovateľovi do 2 000 € ak nezabezpečí dostatočné podmienky pre výkon kontroly a do 10 000 € ak priamo marí výkon kontroly. [37]

2.6 Dozorné orgány

EDPD

„Európska rada pre ochranu údajov (EDPB) je novo vytvorený orgán Európskej únie, ktorý je nezávislý od konkrétneho štátu a ***jeho cieľom je zabezpečiť konzistentné uplatňovanie všeobecného nariadenia o ochrane údajov a európskej smernice o presadzovaní práva v celej Európskej únii.“*** [27]

Úrad na ochranu osobných údajov Slovenskej republiky

„Úrad na ochranu osobných údajov Slovenskej republiky je orgánom štátnej správy s celoslovenskou pôsobnosťou, ktorý vykonáva dozor nad ochranou osobných údajov a podieľa sa na ochrane základných práv a slobôd fyzických osôb pri spracúvaní ich osobných údajov. Pri výkone svojej pôsobnosti postupuje nezávisle a riadi sa ústavou,

ústavnými zákonmi, zákonmi, ostatnými všeobecne záväznými právnymi predpismi a medzinárodnými zmluvami, ktorými je Slovenská republika viazaná.“ [29]

2.7 Súbory Cookies

HTTP Cookie je súbor v textovom formáte, ktorý si webová stránka pri jej návšteve zapíše na pevný disk a pri opakovanom prehliadaní využíva na to, aby zistila spoznala zákaznícku identitu.

Vďaka GDPR, musí obchodník zabezpečiť súlad svojich marketingových aktivít. Nové nariadenie vyžaduje, aby cookies zhromažďovali potvrdzujúci súhlas, ktorý je „slobodne daný, konkrétny, informovaný a jednoznačný.“ [30]

Ich účel sa môže líšiť, ale najčastejší dôvod je:

- Pomáhajú prispôsobiť webovú stránku
- Pomáhajú návštevníkovi navigovať ho cez stránku
- Zlepšujú používateľskú skúsenosť
- Ukladajú preferencie zákazníkov a prihlasovacie informácie
- Relačné cookies, ktoré udržujú užívateľov prihlásených pri prechádzaní webovou stránkou
- Trvalé súbory cookie, ktoré ukladajú prispôsobené predvoľby používateľov
- Súbory cookie, ktoré uchovávajú nákupný košík počas procesu platby [30]

Rozdiel medzi zásadami súborov cookie a zásadami ochrany osobných údajov

Zásady používania súborov cookies sa zaoberajú konkrétne používaním súborov cookie na webe, zatiaľ čo pravidlá ochrany osobných údajov sú všeobecným a komplexným dokumentom poskytujúcim podrobnosti o všetkých procesoch údajov na webových stránkach. [31]

Pravidlá používania súborov cookie môžu byť zvolené ako súčasť väčších pravidiel ochrany osobných údajov. Tento dokument je však rozsiahly a statický, zatiaľ čo povaha súborov cookies sa môže rýchlo meniť vďaka ich schopnosti sledovať, ukladať a zdieľať správanie používateľov. Väčšinu súborov cookie, ktoré sú v prevádzke na webovej stránke, zvyčajne nastavujú tretie strany, čo znamená, že majú iné pravidlá ako samotná webová stránka. [31]

2.8 Kryptovanie

Šifrovanie, je dôležitá časť ochrany osobných údajov. Hoci dáta môžu byť stále ukradnuté, vďaka šifrovaniu ich nie je možné prečítať. Ak zamestnanec stratil zariadenie, v ktorom sa nachádzajú údaje o zákazníkoch (napríklad objednávky, podpora a pod.), alebo ktoré využíva pri práci, vzniká povinnosť zamestnávateľa informovať **všetky dotknuté osoby o strate týchto údajov**. Túto činnosť však vykonať nemusí, ak boli dáta šifrované. Na výber má z dvoch najpoužívanejších možností - **symetrické** a **asymetrické.** [32]

Symetrické šifrovanie používa kombinácie transpozičných alebo substitučných algoritmov. Pointa je v tom , že dva kľúče využité pri šifrovaní sa dajú navzájom odvodiť, čo nie je v tomto prípade vhodný výber - bezpečnosť by závisela len od vhodného chránenia kľúču a pravidelného aktualizovania, nakoľko sa nemôže používať dlhšiu dobu. [32]

Asymetrické šifrovanie používa taktiež dva kľúče, avšak tie na seba nijak nenadväzujú. Šifrovací kľúč sa nazýva „verejný kľúč“ a naopak de-šifrovací má názov „súkromný“, alebo aj „privátny“ kľúč. Útočník musí poznať oba kľúče, aby prelomil ochranu dát. [32]

Dve z najznámejších použití sú :

Šifrovanie verejného kľúča, pri ktorom je správa šifrovaná verejným kľúčom príjemcu. Pre správne zvolené a použité algoritmy nemôžu byť správy v praxi dešifrované kýmkoľvek. Dešifrovať ich môže iba ten, kto má zodpovedajúci súkromný kľúč, o ktorom sa teda predpokladá, že je vlastníkom kľúča, a teda osobou spojenou s verejným kľúčom. To možno použiť na zabezpečenie dôvernosti správy.

Digitálne podpisy, v ktorých je správa podpísaná súkromným kľúčom odosielateľa a môže ich overiť každý, kto má prístup k verejnému kľúču odosielateľa. Toto overenie dokazuje, že odosielateľ mal prístup k súkromnému kľúču, a preto je veľmi pravdepodobné, že bude osobou spojenou s verejným kľúčom. To tiež zaisťuje, že so správou nebolo manipulované, pretože podpis je matematicky viazaný na správu, z ktorej bola pôvodne vyrobená, a overenie zlyhá prakticky pri akejkoľvek inej správe, bez ohľadu na to, ako je pôvodná správa podobná. [32]

2.9 Ukladanie dokumentov

Lehota a spôsob spisovne, archivácie a skartácie dokumentov sa riadi viacerými zákonmi. Konkrétne ustanoveniami § 35,36 zákona č. 431/2002 Z.z. o účtovníctve v znení neskorších predpisov, č. 395/2002 Z. z. o archívoch a registratúrach a o zmene a doplnení niektorých zákonov a vyhlášky Ministerstva vnútra SR č. 628/2002 Z.z..[39]

Spisovný poriadok predstavuje pomôcku pre poverený personál. Pre spisovú službu sa vytvára doručovacia kniha. Do doručovacej knihy sa evidujú všetky prijate písomnosti podľa dátumu obdržania. Dokument sa označí povereným pracovníkom podľa typu odboru, druhu písomnosti, znaku ukladania, lehotou na vyradenie a skartačného znaku. [39]

Archivačný poriadok opisuje prácu s dokumentmi, ktoré sú ešte aktuálne alebo im plynie lehota nutnej archivácie. Ukladajú sa do spisovne a označujú sa podľa spisového poriadku. Spracovateľ musí viesť evidenciu zapožičaní a premiestňovaní týchto dokumentov. **Znakom A** sa označuje archívny registratúrny záznam, ktorý bol posunutý do archivačného procesu. Podľa kritérií sa navrhne potrebná archivačná lehota.[39]

Skartačný poriadok opisuje vyraďovanie písomností podľa spôsobu.

Skartačný znak - označujú sa znakom pred uložením do spisovne. Podľa znakov sa po uplynutí lehôt navrhnú ďalšie postupy.

“A“ znak – archív – po uplynutí lehoty sa dokument prevezme do archívnej sekcie

“**S“ znak** – Skartácia - po uplynutí lehoty sa dokument prevezme do archívnej sekcie

„V“ znak – Výber - po uplynutí lehoty sa rozhodne, či dokument zaradiť do archívnej starostlivosti, alebo odstrániť.[39]

Skartačná lehota určuje dobu, po ktorú dokument stáva uložený v spisovni. Začína plynúť od 1. januára nasledujúceho roka po prijatí dokumentu. Lehoty nemožno skrátiť. [39]

3 VLASTNÝ NÁVRH RIEŠENIA

Spoločnosť aktívne pracuje s OÚ a je nutné, aby sa riadila súčasnou smernicou GDPR. Sama má vypracované a implementované smernice, čo znamená že v tomto návrhu nebude potrebné do nich invazívne zasahovať a meniť štruktúru od základov.

Problém nastáva v tom, že tieto dokumenty boli vytvorené externou firmou a sú neaktuálne. Preto je dôležité zvážiť, či pri implementácii najmúť externú firmu, ktorej pozitívum je bezchybnosť a právna korektnosť, avšak za vysokú cenu a nedostatočný náhľad na firemnú problematiku, alebo poveriť osobu vo firme, ktorá bude mať skúsenosti z vnútorného prostredia a potrebné znalosti pre korektnú implementáciu. Firma by tak stále disponovala poverenou osobou upravovať smernice podľa najnovších zákonov.

3.1 Zavedenie zodpovednej osoby pre kontrolu správnosti postupov GDPR

Spoločnosť nedisponuje zodpovednou osobou za ochranu dát. Právne nepotrebuje osobu DPO, avšak pre jej výhody sa odporúča najať poverená osoba z hľadiska prevencie, ktorá bude zodpovedná za kontrolu a súlad nariadení GDPR s aktuálnymi dokumentmi, správnosť pri pracovných postupoch a pravidelné preškoľovanie zamestnancov.

Podľa predložených dokumentov firmy sa v aktuálnom GDPR spise nachádza bývalá osoba DPO, ktorá už vo firme nemá pracovnoprávnu zmluvu. Je odporúčané takúto osobu bezodkladne najať.

Táto osoba bude zodpovedná za nasledovné body:

1. **Kontrola e-mailu HR** - vytvorenie nového spoločného emailu pre uchádzačov. Tzv, dvojitá kontrola od zamestnanca povereného prijímacími konaniami a zodpovednej osoby.
2. **Neaktuálne znenie smernice** – výmaz chybných informácii a doplnenie aktuálnych najnovších prijatých EDPD.
3. **Plánovanie školení o GDPR**, ich správne implementovanie do praxe.
4. Spolupracovať s jednotlivými oddeleniami a vytvoriť interné smernice.

Smernice budú obsahovať politiku bezpečnosti informácií a to konkrétne:

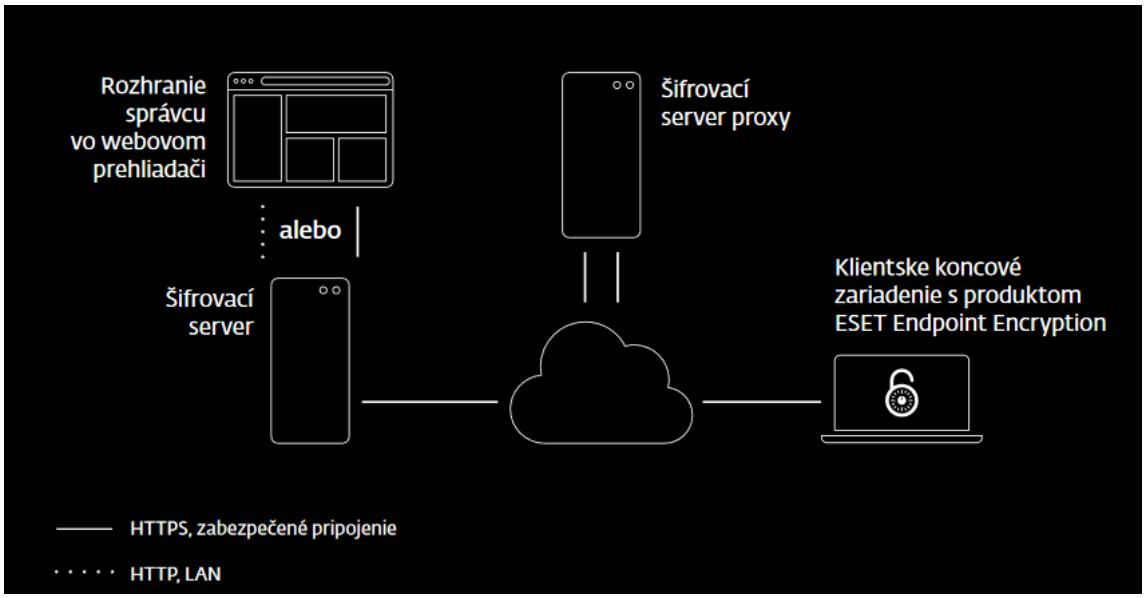
- Ciele, spôsoby a dôvody zabezpečenia OÚ
- Pravidlá emailovej komunikácie tak, aby boli základným pilierom zaúčania nového zamestnanca, robiť pravidelné kontroly
- Šablóny pre najčastejšie situácie, s ktorými sa zákaznícka podpora stretáva
- Politiku mobilných a iných prenosných zariadení
- Bezpečnosť personálu
- Klasifikácia, riadenie a hodnotenie informačných aktív
- Fyzické zaistenie bezpečnosti (zámky, evidenciu kľúčov)
- Spôsoby šifrovania
- Spôsoby zálohovania
- Spôsoby získavania súhlasu GDPR

3.2 Technické opatrenia

Poverená osoba vykoná kompletnú analýzu procesov a postupov v oddeleniach L2 a L3 a na základe výstupu navrhne pravidlá, ktoré tieto postupy a procesy uvedie do súladu so zásadami ochrany osobných údajov s už existujúcimi zásadami ochrany osobných údajov.

3.2.1 Kryptovanie

V súčasnosti firma nedisponuje žiadnym kryptovaním údajov, čo predstavuje riziko. Pre jednoduchšie zavedenie, spoľahlivosť a podporu je odporúčané používať externú službu od spoločnosti **ESET – Endpoint Encription.**



Obrázok 5 Eset Endpoint Encription
(Zdroj: [33])

Eset využíva šifrovanie všetkých dát pevného disku, usb e-mailov a priečinkov, je kompatibilný, spĺňa podmienky aktuálnych štandardov a podporuje najnovšie operačné systémy. Problém môže nastať v správe s linuxovými servermi, preto je potrebné vytvoriť špeciálnu službu, ktorá bude fungovať mimo klasického cenníka. Výhodou je, že všetky služby ESET podliehajú pod metódy schválene NIST-om [33] Ďalšiu výhodu predstavuje obojstranná zmluva. Obe firmy si navzájom poskytujú služby, vďaka čomu sa vytvára jednoduchšia komunikácia a dohoda na cene tejto služby.

Ak by sa technici rozhodli pre vytvorenie kryptovania mimo externého prostredia, vypísaných je niekoľko subjektívnych odporúčaní.

Odporúčania, ktoré majú vykonať technici pri tvorbe kryptovania:

- ✔ Štandardizované schémy, kryptografické algoritmy a protokoly
- ✔ Pravidelná údržba kľúčov a hesiel a ich kontrola
- ✔ Disponovanie profesionálom so znalosťami konfiguračných a kryptografických riešení
- ✔ Plány v prípade kompromitácie údajov – kľúčov a hesiel
- ✔ Použitie funkcie hashovania s dvojnásobnou dĺžkou odtlačku ako je dĺžka symetrického kľúča
- ✔ Pravidelná výmena hesiel [34]

3.2.2 Zálohovanie

Zálohovanie sa robí denne v nočných hodinách. Prebieha každý deň po dobu 14 dní a následne sa robia mesačné snapshoty, ktoré sa ukladajú na dátové úložisko mimo firemnej geolokácie. Chyby v aktuálnom nastavení:

- ✗ Iba 1 úložisko
- ✗ 1 kopia dát
- ✗ Úložisko nie je Online - Vysoké riziko fyzického poškodenia.
- ✗ Posledná záloha iba mesačná
- ✗ Zálohy sú v kombinovanej forme - nekomprimované dáta a snapshoty

Zálohy by mali spĺňať tieto body:

- ✓ Najmenej 3 kópie dát
- ✓ Najmenej 3 rozdielne miesta, z toho aspoň jedno cloudové, NAS a iné dátové centrum
- ✓ Zálohy musia byť šifrované podľa predošlej témy
- ✓ Prechod na kompletne snapshotové zálohovanie - menej priestoru
- ✓ Najmenej mesačné zálohy po dobu pol roka a vždy aspoň jedna ročná záloha. [35]

Firma nedisponuje vnútornými smernicami, ktoré by pokrývali rizikové situácie. V prípade vzniku môže nastať chaotická situácia, kedy zamestnanci nebudú vedieť ako problém riešiť. Odporúča sa vytvoriť vnútorná smernica, resp. postup pre riešenia najčastejších situácii, ktoré ohrozujú dáta a ich prevenciu.

Ďalej sa odporúča aspoň raz ročne umelo vytvoriť túto situáciu a otestovať tak funkčnosť obnovy dát zo záloh v testovacom prostredí.

3.2.3 Sieťový Firewall

Aktuálne funguje len na osobitných systémoch - **hostiteľský firewall**. Preto je dôležité zriadiť aj hlavný – **sieťový firewall vyššej triedy - NGFW**, pre riadenie prístupu do oddelených sietí a ku konkrétnym zariadením. Táto trieda pri kontrole

paketov disponuje funkciami ako prevencia proti útokom, protekcia proti malwarom a spamom.

3.2.4 DLP

V spoločnosti sa pracuje s veľmi citlivými údajmi a preto je potrebné implementovať technológiu DLP - Data loss prevention. Data Loss prevention je efektívny nástroj pre ochranu dát, či ich odcudzeniu.

3.3 Zamestnanci - Prístupy

V kapitole „Zhodnotenie analýzy“ boli označené nehodiace sa práva a prístupy, ktoré majú konkrétne oddelenia. Firma sa plánuje rozrastať na korporáciu a niektoré pracovné posty majú zbytočne práva k osobným údajom zákazníkov, hoci ich pri práci nevyužívajú. Práva preto sú odporúčania na úpravu nasledovne.

Pôvodné práva:

Tabuľka 17 kontrola Prístupov zamestnancov k osobným údajom
(Zdroj: Vlastné spracovanie)

	Technické oddelenie	Obchod	Marketing	Fakturačné oddelenie	Riaditelia	Vedúci oddelení
OÚ zamestnancov						
OÚ zákazníkov						
návštevníci webu						
OÚ dodávateľov						

Tabuľka 18 Legenda vhodnosti
(Zdroj: Vlastné spracovanie)

	Vhodnosť	
Legenda		V poriadku
		Preveriť
		Zlá

Odporučenie úprav prístupov:

Tabuľka 21 úprava prístupov
(Zdroj: Vlastné spracovanie)

	Technické oddelenie	Obchod	Marketing	Fakturačné oddelenie	Riaditelia	Vedúci oddelení
OÚ zamestnancov						
OÚ zákazníkov						
OÚ návštevníkov webu						
OÚ dodávateľov						

3.4 Zákazníci a ich rozhranie

V každom strete zamestnanca/ firmy s osobnými údajmi zákazníka je nutné vytýčiť niekoľko bodov. Dôležité je informovať vopred a to o nasledujúcich záležitostiach:

a) Kto spracováva údaje
b) Prečo spracováva OÚ
c) Akým spôsobom získava OÚ
d) Aký je právny dôvod, účel a rozsah spracovania osobných údajov – Či už marketingové účely, plnenie zákonnej povinnosti, či podľa článku 89 GDPR
e) Aké oprávnene záujmy sú sledovane pri spracúvaní osobných údajov
f) Komu sú sprístupnené OÚ
g) Informácia, po akú dlhú dobu budú uchované OÚ
h) Aké sú práva dotknutej osoby. [36]

3.4.1 Cookies

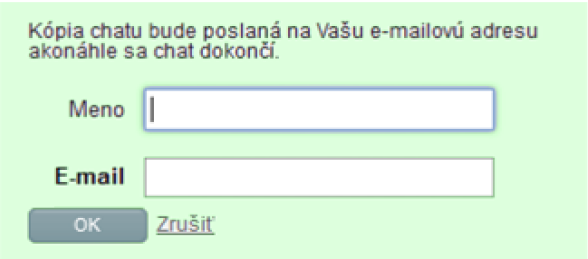
Pri súhlase so súbormi Cookies zákazník nemá možnosť prekliknúť si na podmienky poskytovania jeho osobných údajov. To je v rozpore s niekoľkými pravidlami politiky GDPR. Zákazník musí byť informovaný o údajoch, ktoré poskytuje a tieto podmienky musia byť ľahko dohľadatelné.

Obrázok 6 Súhlas so súbormi Cookies
(Zdroj: Vlastné spracovanie)

1. **Firme je odporúčané vytvoriť samostatný článok o súboroch Cookies. Bude obsahovať:**
    a. Čo Cookies znamenajú
    b. Prečo sa používajú
    c. Konkrétne typy súborov , ktoré sa spracúvajú (Tie so súhlasom)
2. **Súbory musia byť označené v texte (obr. č.15 – zákazník musí byť schopný sa k nim dostať na 1 klik.)**
3. **Zákazník bude vidieť možnosť nesúhlasu.**

3.4.2 Chatovacie okienko

Pri vstupe do chatovacieho okienka program zákazníka vyzve, aby vyplnil svoje meno. Systém nevyžaduje použiť reálnu identitu, však množstvo zákazníkov zadáva svoje skutočné identifikátory a týmto úkonom sa spoja s IP a emailovou adresou daného zákazníka a stáva sa z nich osobný údaj.



Obrázok 7 Informácie o zákazníkovi
(Zdroj: Vlastné spracovanie)

Je nutné, aby zákazník vyjadril súhlas so zadaním týchto údajov. Stačí teda vytvoriť zaškrtávacie políčko, tzv. "checkbox" pre Súhlas s poskytnutím osobných údajov.

3.5 Dokumenty

Z analýzy vyplýva nedostatočné zabezpečenie dokumentov vo fyzickej podobe, ktoré obsahujú OÚ a nakladanie s nimi. Kancelária je typu open-office, a preto je nutné zaobstarať uzamykateľné skrine trezorového typu a vytvoriť sekciu vo vnútornej smernici

o nakladaní s týmito dokumentami. Prípadne zvoliť možnosť digitalizácie a nahranie do informačného systému Ekonix. V prípade ponechania fyzickej formy dokumentu bude vytvorená smernica obsahovať:

- Osoby zodpovedné za dodržiavanie smernice
- Nariadenie o uzamykaní fyzického úložiska
- Dokumenty môžu byť vyňaté len na určitý časový úsek a to po dobu nutnú pre prácu s týmito dokumentami oprávnenou osobou
- Všetky dokumenty musia byť evidované s kompletným životným cyklom, vrátane údajov o dĺžke legálneho držania a dôvody jeho držania.
- Stanovený pravidelný dátum kontroly dokumentov (aktuálnosť a pominutie dôvodu držania dokumentu)
- Pravidlá zničenia (skartácie) dokumentov a odkaz na ustanovenia schváleného registratúrneho poriadku a skartačného postupu.
- Pri každej zmluve bude osobitný súhlas so spracovaním osobných údajov, podľa § 14 Podmienok poskytnutia súhlasu so spracúvaním osobných údajov.

Ak zmluva, fyzická, či digitálna, neobsahuje súhlas o uchovávaní osobných údajov, musí byť bezodkladne zničená.

3.5.1 Archivácia a skartácia

Firma je povinná sa riadiť skartačným archivačným a spisovným poriadkom. Dokumenty je odporúčané ukladať nielen podľa konkrétnych znakov A,S,V ale aj s konkrétnym číslom plynúcej lehoty. Napr. v prípade Archívneho dokumentu označiť písomnosť „A5“ , ktorá by určovala 5 ročnú lehotu držania dokumentu. Skartačné obdobie bude prebiehať raz ročne, a bude sa viesť evidencia poverených pracovníkov ktorá bude uložená v spisovni – v trezore, alebo skrini. Smernica bude obsahovať skartačný a spisovný plán ako papierových dokumentov, rovnako aj digitálnych dokumentov. [39]

Tabuľka 22 Príklad dokumentácie písomnosti
(Vzor: [39])

Druh dokumentu	Označenie
Evidencia predaja (fakturácia)	S5
Obchodné zmluvy	V10

ZÁVER

V tejto bakalárskej práci sme sa venovali zákonu o ochrane osobných údajov a jeho aplikovaní vo firme poskytujúcej hostingové služby. Mojou úlohou bolo nielen preveriť aktuálne dokumenty a smernice v existujúcej zabehnutej firme, ale taktiež vytýčiť problémy a chyby a apelovať na ich správnu nápravu. V analýze firmy sa dopodrobna urobil rozbor existujúcej hostingovej firmy Web-net. s.r.o., vďaka čomu sme ľahšie mohli určiť, aké dáta firma spracováva a na základe toho vyvodiť subjektívny názor na aktuálne zabezpečenie údajov vo firme.

V teoretickej časti boli deduktívnou metódou opísané podstatné súčasti práce od informácie, až po jej možnosti zneužitia v podnikaní a na základe toho vzniknutý zákon ochrany osobných údajov, ktoré poskytli práci podporný materiál, pre dokazovanie nutnosti zavedenia návrhov v ďalšej kapitole. V poslednej kapitole návrhových riešení bola preverená každá situácia, v ktorej ochrana osobných údajov nebola dostačujúca a poskytnutá adekvátna alternatíva a aktualizácia tak, aby v súčasnosti a budúcnosti netvorili problém so zákonom a jeho vyhláškami. Pre jednoduchšiu orientáciu som v posledných stranách mojej práce zverejnila zdroje literatúry, zoznam obrázkov a tabuliek a prílohy pre jednoduchšie dokazovanie mojich zistení. Ciele považujem za úspešne splnené a verím, že tak ako ja, aj firma budeme z týchto nadobudnutých informácii čerpať pri tvorbe novej smernice.

Práca pre mňa bola naozaj prínosom, nielen že som sa naučila zbierať množstvo informácii o konkrétnej problematike, taktiež ma donútila témou zaoberať sa naozaj do hĺbky. Po zrealizovaní tejto práce som omnoho viac obozretnejšia, k čomu dávam môj súhlas nielen v pracovnom prostredí, ale aj v online priestore rôznym stránkam.

ZOZNAM SKRATIEK A VÝRAZOV

GDPR – General Data Protection Regulation

HO – Home Office

Single Point of Failiure – Bod zlyhania systému – jeho zlyhanie zastaví celý proces

Cloud – Typ úložného priestoru

GeoIp – geolokácia

NIST – Národný Inštitút pre štandardy a technológie

VPN – Virtuálna privátna sieť

Open office – pracovisko s otvoreným priestranstvom

ZOZNAM OBRÁZKOV

ZOZNAM TABULIEK

ZOZNAM POUŽITEJ LITERATÚRY

[1] Infraštruktúra. *Wy.sk* [online]. [cit. 2021-4-29]. Dostupné z: https://wy.sk/o-wy/infrastruktura/

[2] Článok 4 EÚ všeobecné nariadenie o ochrane údajov "Vymedzenie pojmov"

[3] MIKLOŠOVÁ, PhDr. Anna. Smernica na ochranu osobných údajov od 25.5.2018. *Zoou.sk* [online]. 24.5.2018, , 49 [cit. 2021-04-06]. Dostupné z: https://www.zoou.sk/33/smernica-na-ochranu-osobnych-udajov-od-25-5-2018-uniqueidmRRWSbk196FPkyDafLfWAJWc7pG-Xzb6jpsj_iqtBV-CPYj7CkleJQ/

[4] Informačný systém osobných údajov. *Dataprotection.gov.sk* [online]. [cit. 2021-4-29]. Dostupné z: https://dataprotection.gov.sk/uoou/sk/content/informacny-system-osobnych-udajov

[5] *Chat* [online]. *Techterm.com* [online]. [cit. 2021-4-26]. Dostupné z: https://techterms.com/definition/Chat

[6] *Hosting* [online]. *Techterm.com* [online]. [cit. 2021-4-26]. Dostupné z: https://techterms.com/definition/hosting

[7] *Snapshot* [online]. *Techterm.com* [online]. [cit. 2021-4-26]. Dostupné z: https://techterms.com/definition/snapshot

[8] *Server* [online]. *Techterm.com* [online]. [cit. 2021-4-26]. Dostupné z: https://techterms.com/definition/server

[9] *Hacker* [online]. *Techterm.com* [online]. [cit. 2021-4-26]. Dostupné z: https://techterms.com/definition/hacker

[10] *Raid* [online]. *Techterm.com* [online]. [cit. 2021-4-26]. Dostupné z:raid

[11] *Zodpovedná osoba* [online]. *Dataprotection.gov.sk* [online]. [cit. 2021-4-26]. Dostupné z: https://dataprotection.gov.sk/uoou/sk/content/zodpovedna-osoba-0

[12] *Cookies* [online]. [cit. 2021-4-26]. Dostupné z: https://techterms.com/definition/Cookies

[13] *SSL* [online]. [cit. 2021-4-26]. Dostupné z: https://techterms.com/definition/SSL

[14] BUCKLAND, Michael. *Information and Information Systems*. Westport, Spojené Štáty Americké: ABC-CLIO, 2000, 248 s. ISBN 978-02-7593-851-2.

[15] HUČKOVÁ, Regina, D. TREŠČÁKOVÁ a L. RÓZENFELDOVÁ. *Právo informačných a komunikačných technológií*. Košice: Univerzita Pavla Jozefa Šafárika v Košiciach, 2020. ISBN 978-80-8152-910-8.

[16] Rozdelenie osobných údajov. iapp.org [online]. [cit. 2021-4-26]. Dostupné z: https://iapp.org/resources/article/categories-of-personal-data/

[17] Článok 6 EÚ všeobecné nariadenie o ochrane údajov "Zákonnosť spracúvania"

[18] ZIMEN, Ondrej. GDPR - Časť 1: Najzásadnejšie zmeny. *Steiniger.sk* [online]. 5.2.2017 [cit. 2021-04-06]. Dostupné z: https://www.steinigers.sk/gdpr-cast-1-najzasadnejsie-zmeny

[19] Čo je GDPR? *Gdpr-slovensko.sk* [online]. [cit. 2021-4-29]. Dostupné z: https://gdpr-slovensko.sk/co-je-gdpr/

[20] PRISPIEVATELIA WIKIPÉDIE. Všeobecná deklarácia ľudských práv. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001-, 12.2.2021 [cit. 2021-04-06]. Dostupné z: https://sk.wikipedia.org/w/index.php?title=V%C5%A1eobecn%C3%A1_deklar%C3%A1cia_%C4%BEudsk%C3%BDch_pr%C3%A1v&oldid=7160124

[21] PRISPIEVATELIA WIKIPÉDIE. Dohovor o ochrane ľudských práv a základných slobôd. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 26.8.2019 [cit. 2021-04-06]. Dostupné z: https://sk.wikipedia.org/w/index.php?title=Dohovor_o_ochrane_%C4%BEudsk%C3%BDch_pr%C3%A1v_a_z%C3%A1kladn%C3%BDch_slob%C3%B4d&oldid=6886326

[22] EUROPEAN DATA PROTECTION SUPERVISOR. The History of the General Data Protection Regulation. *Edps.europa.eu* [online]. [cit. 2021-04-

06]. Dostupné z: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

[23] PRISPIEVATELIA WIKIPÉDIE. Všeobecné nariadenie o ochrane údajov. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001-, 14.8.2020 [cit. 2021-04-06]. Dostupné z: https://sk.wikipedia.org/w/index.php?title=V%C5%A1eobecn%C3%A9_nariadenie_o_ochrane_%C3%BAdajov&oldid=7075309

[24] Zákon č. 18/2018 Z. z. Zákon o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

[25] MATOUŠOVÁ, Miroslava. *Osobní údaje a jejich ochrana: knížka pro praxi*. Praha: ASPI, 2003. ISBN 80-86395-50-2.

[26] EUROPEAN COMMISSION. What is a data controller or a data processor? *Ec.europa.eu* [online]. [cit. 2021-04-06]. Dostupné z: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en

[27] Dotknuté osoby. *Dataprotection.gov.sk* [online]. [cit. 2021-4-26]. Dostupné z: https://dataprotection.gov.sk/uoou/sk/content/dotknuta-osoba

[28] Kto sme. *Edpb.europa.eu* [online]. [cit. 2021-4-29]. Dostupné z: https://edpb.europa.eu/about-edpb/about-edpb_sk

[29] Úrad na ochranu osobných údajov Slovenskej republiky. *dataprotection.gov.sk* [online]. [cit. 2021-4-29]. Dostupné z: https://dataprotection.gov.sk/uoou/sk/content/urad

[30] MCCARTHY, Linda a D. WELDON-SIVIY. *Buď pánem svého prostoru: jak chránit sebe a své věci, když jste online*. Praha: CZ.NIC, 2013. ISBN 978-80-904248-6-9.

[31] Adding Privacy Policy and Terms of Service. Yola.com [online]. [cit. 2021-04-06]. Dostupné z: https://www.yola.com/tutorials/article/How-to-add-a-Privacy-Policy-and-Terms-of-Service/GDPR_Compliance_and_Legal_Pages

[32] STINSON, Douglas a Maura PATERSON. *Cryptography: Theory and Practice*. 4. Boca Raton,Florida: CRC Press, 2018 [cit. 2021-04-06]. ISBN 978-1138197015.

[33] Ochrana identity a údajov. *Eset.com* [online]. [cit. 2021-4-29]. Dostupné z: https://www.eset.com/sk/firemna-it-bezpecnost/riesenia/ochrana-identity-a-udajov/

[34] TANEK Martin a M. Rajško. Kryptológia. In: Csirt.sk [online]. [cit. 2021-4-29]. Dostupné z: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwj02N6DoKPwAhXSl4sKHTqLBdwQFjAEegQIDxAD&url=https%3A%2F%2Fwww.csirt.gov.sk%2Fdoc%2FMFSRVzdelavanie%2F02Vzdelavanie2014%2FPrezentacie_specialisti_na_informacnu_bezpecnost%2FPrezS_2014_02_Kryptologia.pdf&usg=AOvVaw2p0Ir-nxCYGDgzGxhM0u0j

[35] Zálohovanie dát. *Alza.sk* [online]. [cit. 2021-4-29]. Dostupné z: https://www.alza.sk/zalohovanie-dat#tipy-triky

[36] Článok 13 EÚ všeobecné nariadenie o ochrane údajov "Informácie, ktoré sa majú poskytovať pri získavaní osobných údajov od dotknutej osoby"

[37] Dôvodová tlač k zákonu č. 18/2018 Z.z. Dátum publikácie 30.1. 2018

[38] HECKO, Zuzana a Porubský M. Slovensko ako priekopník v „preklápaní“ nariadenia GDPR do zákona. *Allenovery.com* [online]. 2017 [cit. 2021-5-10]. Dostupné z: https://www.allenovery.com/en-gb/global/news-and-insights/publications/slovensko-ako-priekopnik-v-preklapani-nariadenia-gdpr-do-zakona?fbclid=IwAR2GLeBi0kd3apzA5KdavYkEO_ws-u34XNQgLQDDujuWU7fo45IrUjCMHIA

[39] MAJOROVÁ, Ing. Miriam. Smernica upravujúca spisový, archívny, a skartačný poriadok účtovných písomností a účtovných záznamov. *uad.sk* [online]. 10.1.2020 [cit. 2021-5-13]. Dostupné z: https://www.uad.sk/33/smernica-upravujuca-spisovy-archivny-a-skartacny-poriadok-uctovnych-pisomnosti-a-uctovnych-zaznamov-v-po-uniqueidmRRWSbk196FPkyDafLfWAMMzOZNTKFrQt7T6eB6ygDhnXUf-iNv8cQ/

PRÍLOHY

[1] Príloha zmluvy o spracúvaní osobných údajov

[2] Súhlas zamestnanca so spracúvaním fotografie